STAATSCOURANT
Officiële uitgave van het Koninkrijk der Nederlanden sinds 1814.
Nr. 46128
16 december
2015

# De meldplicht datalekken in de Wet bescherming persoonsgegevens (Wbp)

Beleidsregels voor toepassing van artikel 34a van de Wbp

## Samenvatting

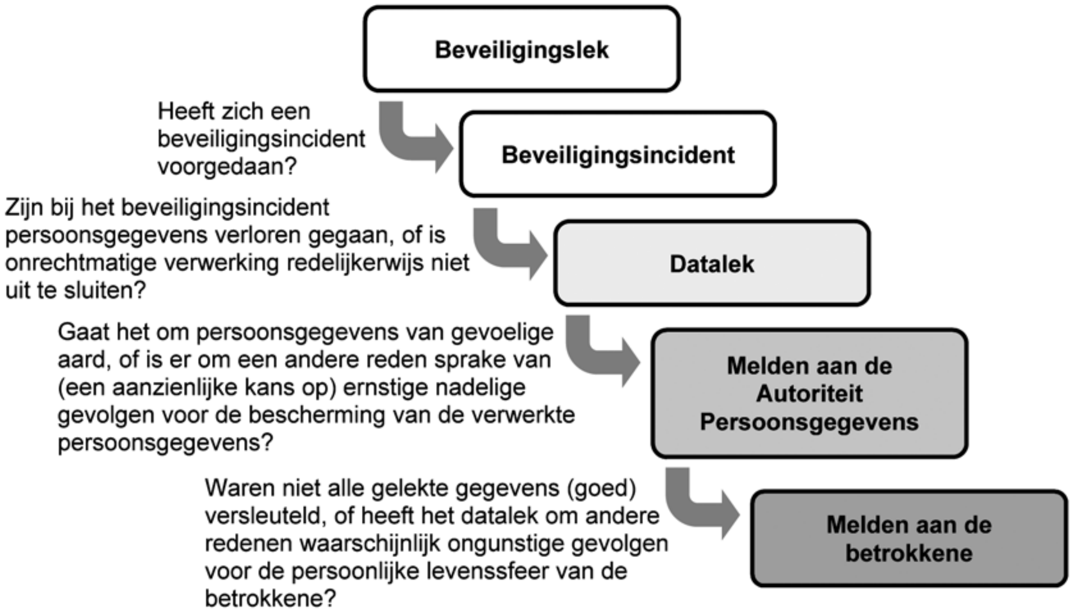
Op 1 januari 2016 gaat de meldplicht datalekken in. Deze meldplicht houdt in dat organisaties (zowel bedrijven als overheden) onverwijld een melding moeten doen bij de Autoriteit Persoonsgegevens zodra zij een ernstig datalek hebben. En in een aantal gevallen moeten zij het datalek ook melden aan de betrokkenen (de mensen van wie de persoonsgegevens zijn gelekt).

### *Kader*

Iedereen heeft recht op eerbiediging en bescherming van zijn persoonlijke levenssfeer en een zorgvuldige omgang met zijn persoonsgegevens. De regels hiervoor zijn vastgelegd in de Wet bescherming persoonsgegevens (Wbp). Hierin staat dat u de persoonsgegevens die u verwerkt moet beveiligen tegen verlies en tegen onrechtmatige verwerking (artikel 13 Wbp). Een datalek moet worden gemeld aan de Autoriteit Persoonsgegevens als het leidt tot een aanzienlijke kans op ernstige nadelige gevolgen voor de bescherming van persoonsgegevens, of als het ernstige nadelige gevolgen heeft voor de bescherming van persoonsgegevens (artikel 34a, eerste lid, Wbp). Het datalek moet daarnaast ook worden gemeld aan de betrokkene indien het waarschijnlijk ongunstige gevolgen zal hebben voor diens persoonlijke levenssfeer (artikel 34a, tweede lid, Wbp).

### *Afwegingen*

Bij de beslissing of u een gebeurtenis die zich heeft voorgedaan moet melden aan de Autoriteit Persoonsgegevens, en eventueel daarnaast ook aan de betrokkene, moet u een aantal afwegingen maken. Het onderstaande schema geeft deze afwegingen weer.




### *Datalek*

Er is alleen sprake van een datalek als zich daadwerkelijk een beveiligingsincident heeft voorgedaan. Bij een beveiligingsincident moet u bijvoorbeeld denken aan het kwijtraken van een USB-stick, de diefstal van een laptop of aan een inbraak door een hacker.

Maar niet ieder beveiligingsincident is ook een datalek. Er is sprake van een datalek als er bij het beveiligingsincident persoonsgegevens verloren zijn gegaan, of als u onrechtmatige verwerking van de persoonsgegevens niet redelijkerwijs kunt uitsluiten.

Als alleen sprake is van een zwakke plek in de beveiliging, spreken we van een beveiligingslek en niet van een datalek. U hoeft dan geen melding te doen aan de Autoriteit Persoonsgegevens.

### *Melden aan de Autoriteit Persoonsgegevens*

U hoeft niet ieder datalek te melden aan de Autoriteit Persoonsgegevens. Volgens de wet moet u een melding doen aan de Autoriteit Persoonsgegevens als het datalek leidt tot een aanzienlijke kans op ernstige nadelige gevolgen voor de bescherming van persoonsgegevens, of als het ernstige nadelige gevolgen heeft voor de bescherming van persoonsgegevens.

Een factor die hierbij een rol speelt is de aard van de gelekte persoonsgegevens. Als er persoonsgegevens van gevoelige aard zijn gelekt, dan is over het algemeen een melding noodzakelijk. Bij persoonsgegevens van gevoelige aard moet u denken aan:

- *Bijzondere persoonsgegevens zoals bedoeld in artikel 16 Wbp*
  Het gaat hierbij om persoonsgegevens over iemands godsdienst of levensovertuiging, ras, politieke gezindheid, gezondheid, seksuele leven, lidmaatschap van een vakvereniging en om strafrechtelijke persoonsgegevens en persoonsgegevens over onrechtmatig of hinderlijk gedrag in verband met een opgelegd verbod naar aanleiding van dat gedrag.
- *Gegevens over de financiële of economische situatie van de betrokkene*
  Hieronder vallen bijvoorbeeld gegevens over (problematische) schulden, salaris- en betalingsgegevens.
- *(Andere) gegevens die kunnen leiden tot stigmatisering of uitsluiting van de betrokkene*
  Hieronder vallen bijvoorbeeld gegevens over gokverslaving, prestaties op school of werk of relatieproblemen.
- *Gebruikersnamen, wachtwoorden en andere inloggegevens*
  De mogelijke gevolgen voor betrokkenen hangen af van de verwerkingen en van de persoonsgegevens waar de inloggegevens toegang toe geven. Bij de afweging moet worden betrokken dat veel mensen wachtwoorden hergebruiken voor verschillende verwerkingen.
- *Gegevens die kunnen worden misbruikt voor (identiteits)fraude*
  Het gaat hierbij onder meer om biometrische gegevens, kopieën van identiteitsbewijzen en om het Burgerservicenummer (bsn).

Ook andere factoren, zoals de hoeveelheid gelekte persoonsgegevens per persoon of het aantal betrokkenen van wie er persoonsgegevens zijn gelekt, kunnen aanleiding zijn om het datalek te melden. Maar let op: als de aard van de gelekte gegevens daar aanleiding toe geeft is het mogelijk dat u een datalek moet melden waar de persoonsgegevens van slechts één persoon bij betrokken zijn.

U moet de melding doen zonder onnodige vertraging en zo mogelijk niet later dan 72 uur na de ontdekking van het datalek. Op de website van de Autoriteit Persoonsgegevens is voor dit doel een webformulier beschikbaar. Via dit webformulier kunt u de melding zo nodig aanvullen of intrekken.

### *Melden aan de betrokkene*

Als u tot de conclusie komt dat u een datalek moet melden aan de Autoriteit Persoonsgegevens, dan betekent dit niet automatisch dat u dit datalek ook moet melden aan de betrokkene. U moet hiervoor een aparte afweging maken.

De wet geeft aan dat u een melding moet doen aan de betrokkene als het datalek waarschijnlijk ongunstige gevolgen zal hebben voor diens persoonlijke levenssfeer. Betrokkenen kunnen door het verlies, onrechtmatig gebruik of misbruik in hun belangen worden geschaad. Daarbij moet u bijvoorbeeld denken aan onrechtmatige publicatie, aantasting in eer en goede naam, (identiteits)fraude of discriminatie. Als er persoonsgegevens van gevoelige aard zijn gelekt, dan kunt u er in principe van uit gaan dat u het datalek niet alleen moet melden aan de Autoriteit Persoonsgegevens, maar ook aan de betrokkene.

Uw melding stelt de betrokkene in staat om alert te zijn op de mogelijke gevolgen van het datalek en om zich daar waar mogelijk tegen te wapenen door, bijvoorbeeld, een gelekt wachtwoord te vervangen. De wet schrijft voor dat u de melding *onverwijld* moet doen. U moet daarbij rekening houden met het feit dat de betrokkene naar aanleiding van uw melding mogelijk maatregelen moet nemen om zich te beschermen tegen de gevolgen van het datalek. Hoe eerder u de betrokkene daarover informeert, hoe eerder deze in actie kan komen.

Als u passende technische beschermingsmaatregelen heeft genomen waardoor de persoonsgegevens die het betreft onbegrijpelijk of ontoegankelijk zijn voor onbevoegden, dan kunt u de melding aan de betrokkene achterwege laten. Bij deze beschermingsmaatregelen moet u bijvoorbeeld denken aan cryptografische bewerkingen zoals encryptie en hashing. U moet per geval bepalen of de maatregelen

die u heeft genomen voldoende bescherming bieden om de melding aan de betrokkene achterwege te kunnen laten.

### *Uitzonderingen op de meldplicht*

De meldplicht datalekken uit de Wbp is niet van toepassing als de Wbp niet van toepassing is. Dit is bijvoorbeeld het geval als u uitsluitend voor persoonlijke of huishoudelijke doeleinden persoonsgegevens verwerkt.

Als u een aanbieder van een openbare elektronische communicatiedienst bent, dan heeft u te maken met twee meldplichten voor datalekken: de meldplicht in de Telecommunicatiewet (Tw) en de meldplicht in de Wbp. Valt een datalek (gedeeltelijk) onder de meldplicht datalekken uit de Tw? Ook dan moet u het datalek melden aan de Autoriteit Persoonsgegevens en mogelijk aan de betrokkene. In de Wbp zijn voorzieningen opgenomen om dubbele meldingen te voorkomen.

Als u een financiële onderneming bent zoals bedoeld in de Wet op het financieel toezicht (Wft), dan is de verplichting uit de Wbp om datalekken te melden aan de betrokkene niet op u van toepassing. Als u de betrokkenen informeert, doet u dat op grond van uw zorgplicht als financiële onderneming.

### *Boete*

Bij overtreding van de meldplicht datalekken uit de Wbp kan de Autoriteit Persoonsgegevens een bestuurlijke boete opleggen. Deze bestuurlijke boete bedraagt ten hoogste het bedrag van de zesde categorie van artikel 23, vierde lid, van het Wetboek van Strafrecht. Dat is per 1 januari 2016 maximaal 820.000 euro.[1] Indien de overtreding niet opzettelijk is gepleegd en er geen sprake is van ernstig verwijtbare nalatigheid, dan zal de Autoriteit Persoonsgegevens eerst een bindende aanwijzing opleggen voorafgaand aan eventuele oplegging van een bestuurlijke boete. Bij het opleggen van een bestuurlijke boete houdt de Autoriteit Persoonsgegevens rekening met alle omstandigheden van het geval. Een omstandigheid van het geval kan bestaan uit het feit dat de gegevens waarover het gaat niet door derden zijn ingezien.

## Inleiding

Met ingang van 1 januari 2016 treedt een wijziging van de Wet bescherming persoonsgegevens (Wbp) in werking die een meldplicht regelt voor datalekken. Deze meldplicht houdt in dat bedrijven, overheden en andere organisaties die persoonsgegevens verwerken datalekken moeten melden aan de Autoriteit Persoonsgegevens, en in bepaalde gevallen ook aan de betrokkene. De betrokkene is degene van wie persoonsgegevens zijn gelekt.

De bedrijven, overheden en andere organisaties tot wie de meldplicht datalekken zich richt moeten zelf een beredeneerde afweging maken of een concreet datalek dat hen ter kennis komt onder het bereik van de wettelijke meldplicht valt. Doel van deze beleidsregels is om hen daarbij te ondersteunen.[2] Deze beleidsregels dienen tevens als uitgangspunt voor de Autoriteit Persoonsgegevens bij het toepassen van handhavende maatregelen.

Deze beleidsregels gaan in op de meldplicht datalekken die is opgenomen in de Wbp. Aanbieders van openbare elektronische communicatiediensten hebben te maken met twee meldplichten voor datalekken: de onderhavige meldplicht, en de al langer bestaande meldplicht voor datalekken die is opgenomen in de Telecommunicatiewet (Tw). De meldplicht datalekken in de Tw komt voort uit Europese regelgeving, en de Europese verordening 611/2013 vult de regels uit deze meldplicht nader in. Onder meer geeft deze verordening aan op welke termijn een datalek aan de toezichthouder moet worden gemeld, welke informatie daarbij moet worden verstrekt en hoe de betrokkene moet worden geïnformeerd over het datalek. Verder is de meldplicht aan de betrokkene door de samenwerkende Europese privacy-toezichthouders nader uitgewerkt in een advies, met daarin een aantal uitvoerig geannoteerde voorbeelden.[3] Deze beleidsregels gaan niet inhoudelijk in op de meldplicht uit de Tw. Wel sluiten deze beleidsregels waar mogelijk aan op de bestaande invulling van deze meldplicht.

Deze beleidsregels treden in werking met ingang van 1 januari 2016, zijnde de datum van inwerkingtreding van de meldplicht datalekken.

---

[1] De bedragen in artikel 23, vierde lid, van het Wetboek van Strafrecht worden elke twee jaar aangepast aan de ontwikkeling van de consumentenprijsindex. Dit betekent dat per 1 januari 2018 een ander bedrag kan gelden.

[2] Kamerstukken II 2014/15, 33 662, nr. 11, blz. 2.

[3] Artikel 29-Werkgroep, Advies 03/2014 over kennisgeving bij inbreuken in verband met persoonsgegevens, goedgekeurd op 25 maart 2014.

In de loop van 2017, of wanneer het aantal ontvangen meldingen daar aanleiding toe geeft, zullen deze beleidsregels worden geëvalueerd en waar nodig aangepast. Er zal dan opnieuw een consultatie plaatsvinden.

Meer informatie over de beveiliging van persoonsgegevens en over de meldplicht voor datalekken vindt u op de website van de Autoriteit Persoonsgegevens.[4]

## Leeswijzer

Het onderstaande schema geeft per onderwerp de relevante hoofdstukken in deze beleidsregels weer.

**Voorbereid zijn op de meldplicht**

| Vraag | Hoofdstuk |
|---|---|
| Is de meldplicht uit de Wbp op mij van toepassing? | **Hoofdstuk 1, blz. 11-15** |
| Wat moet ik regelen als ik persoonsgegevens laat bewerken door een bewerker? | **Hoofdstuk 2, blz. 16-18** |

**Melden of niet?**

| Vraag | Hoofdstuk |
|---|---|
| Is dit een datalek? | **Hoofdstuk 3, blz. 19-22** |
| Moet ik dit datalek melden aan de Autoriteit Persoonsgegevens? | **Hoofdstuk 4, blz. 23-29** |
| Moet ik dit datalek melden aan de betrokkene? | **Hoofdstuk 7, blz. 32-42** |

**Melden aan de Autoriteit Persoonsgegevens**

| Vraag | Hoofdstuk |
|---|---|
| Hoe moet ik het datalek melden aan de Autoriteit Persoonsgegevens? | **Hoofdstuk 5, blz. 30** |
| Wanneer moet ik het datalek melden aan de Autoriteit Persoonsgegevens? | **Hoofdstuk 6, blz. 31** |

**Melden aan de betrokkene**

| Vraag | Hoofdstuk |
|---|---|
| Hoe moet ik het datalek melden aan de betrokkene? | **Hoofdstuk 8, blz. 43-44** |
| Wanneer moet ik het datalek melden aan de betrokkene? | **Hoofdstuk 9, blz. 45** |

**Na de melding**

| Vraag | Hoofdstuk |
|---|---|
| Welke gegevens moet ik vastleggen over dit datalek? | **Hoofdstuk 10, blz. 46-47** |
| Wat doet de Autoriteit Persoonsgegevens met mijn melding? | **Hoofdstuk 11, blz. 48-50** |

Behalve de onderdelen die in het bovenstaande schema zijn weergegeven, bevatten deze beleidsregels een aantal bijlagen. In bijlage 1 bij deze beleidsregels vindt u een overzicht aan van de gegevens

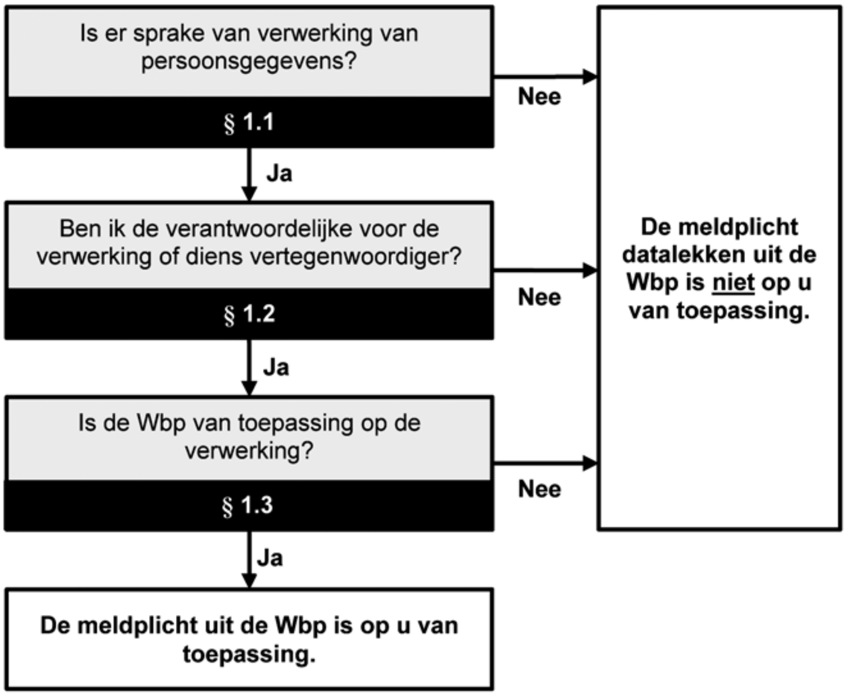
[4] autoriteitpersoonsgegevens.nl.

die u in de melding moet verstrekken. Bijlage 2 geeft de volledige tekst weer van de wetsartikelen die in deze beleidsregels worden geciteerd.

Waar in deze beleidsregels wordt gesproken over de 'meldplicht uit de Wbp' wordt gedoeld op de meldplicht datalekken die is opgenomen in artikel 34a Wbp en waaraan wordt gerefereerd in artikel 14 Wbp, en niet op de meldplicht voor verwerkingen van persoonsgegevens uit de artikelen 27, 28, 29 en 30 Wbp.

## 1. Is de meldplicht datalekken uit de Wbp op mij van toepassing?

Het onderstaande schema geeft de vragen weer die u moet beantwoorden om vast te stellen of de meldplicht datalekken uit de Wbp op u van toepassing is. Iedere vraag uit het schema correspondeert met een paragraaf uit het vervolg van dit hoofdstuk.




In dit hoofdstuk worden begrippen zoals 'persoonsgegevens', 'verwerking' en 'verantwoordelijke' gebruikt. Deze termen uit de Wbp worden in de volgende paragrafen kort toegelicht. Meer informatie over de Wbp en over de betekenis van deze termen vindt u op de website van de Autoriteit Persoonsgegevens.[5]

### *1.1. Is er sprake van verwerking van persoonsgegevens?*

Als er geen sprake is van verwerking van persoonsgegevens, dan is de meldplicht datalekken niet van toepassing.

Een persoonsgegeven is elk gegeven betreffende een geïdentificeerde of identificeerbare persoon (artikel 1, sub a, Wbp). Een persoon is identificeerbaar indien zijn identiteit redelijkerwijs, zonder onevenredige inspanning, vastgesteld kan worden. Er kan een onderscheid worden gemaakt in direct en indirect identificerende gegevens. Direct identificerende gegevens zijn gegevens die betrekking hebben op een persoon waarvan de identiteit zonder veel omwegen eenduidig is vast te stellen, zoals een naam, eventueel in combinatie met het adres en de geboortedatum. Van indirect identificerende gegevens is sprake wanneer gegevens via nadere stappen in verband kunnen worden gebracht met een bepaalde persoon.

Een gegeven is geen persoonsgegeven, indien doeltreffende technische en organisatorische maatregelen zijn getroffen waardoor een daadwerkelijke identificatie van individuele natuurlijke personen redelijkerwijs wordt uitgesloten (anonimisering).

[5] autoriteitpersoonsgegevens.nl.

Het toepassen van cryptografische bewerkingen zoals encryptie of hashing op identificerende gegevens leidt tot pseudonimisering (het vervangen van een identificerend gegeven door een ander identificerend gegeven) maar niet tot anonimisering. Een voorbeeld van een dergelijke bewerking is het versleutelen of hashen van klantnummers. Als verantwoordelijke bent u, ook na de encryptie of hashing, nog steeds in staat om de betrokkene te identificeren. Er is dus nog steeds sprake van persoonsgegevens. Wel is pseudonimisering een waardevolle beveiligingsmaatregel die bij een datalek de kans op daadwerkelijk misbruik van de gelekte persoonsgegevens aanzienlijk kan verlagen.

Het verwijderen van de direct identificerende gegevens biedt op zichzelf niet altijd voldoende garantie dat er geen sprake meer is van persoonsgegevens. Door middel van spontane herkenning, vergelijking van gegevens en/of koppeling aan gegevens uit een andere bron, kan immers desondanks, soms zonder bijzondere inspanning, identificatie tot stand worden gebracht. Verder moet bij anonimisering rekening worden gehouden met de stand van de techniek. Wat bij een bepaalde stand van de techniek als anoniem kan worden beschouwd, aangezien het gegeven niet redelijkerwijs tot een persoon te herleiden is, kan door technische ontwikkelingen alsnog een persoonsgegeven worden gelet op de toegenomen mogelijkheden tot herleiding.

Verwerking van persoonsgegevens betreft elke handeling of elk geheel van handelingen met betrekking tot persoonsgegevens. Hieronder valt in ieder geval het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van gegevens (artikel 1, sub b, Wbp).

### *1.2. Ben ik de verantwoordelijke voor de verwerking of diens vertegenwoordiger?*

De meldplicht datalekken richt zich tot de verantwoordelijke voor de verwerking van persoonsgegevens.

De verantwoordelijke is degene die, alleen of tezamen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt (artikel 1, sub d, Wbp). Het gaat hierbij om de vraag wie uiteindelijk bepaalt welke verwerking er plaatsvindt van welke persoonsgegevens en voor welk doel. Ook is van belang wie er beslist over de middelen voor die verwerking: de vraag op welke manier de gegevensverwerking zal plaatsvinden. Deze bevoegdheden kunnen soms in verschillende handen liggen. In dat geval is er sprake van gezamenlijke verantwoordelijkheid.

Als een verantwoordelijke van buiten de Europese Unie persoonsgegevens verwerkt, en de Wbp van toepassing is op deze verwerking, dan moet de verantwoordelijke in Nederland een persoon of instantie aanwijzen die namens hem de verplichtingen uit de Wbp nakomt. Voor de toepassing van de Wbp en de daarop berustende bepalingen, wordt deze persoon of instantie aangemerkt als de verantwoordelijke.

### *1.3. Is de Wbp van toepassing op de verwerking?*

De meldplicht datalekken uit de Wbp is uitsluitend van toepassing op verwerkingen waarop de Wbp van toepassing is.

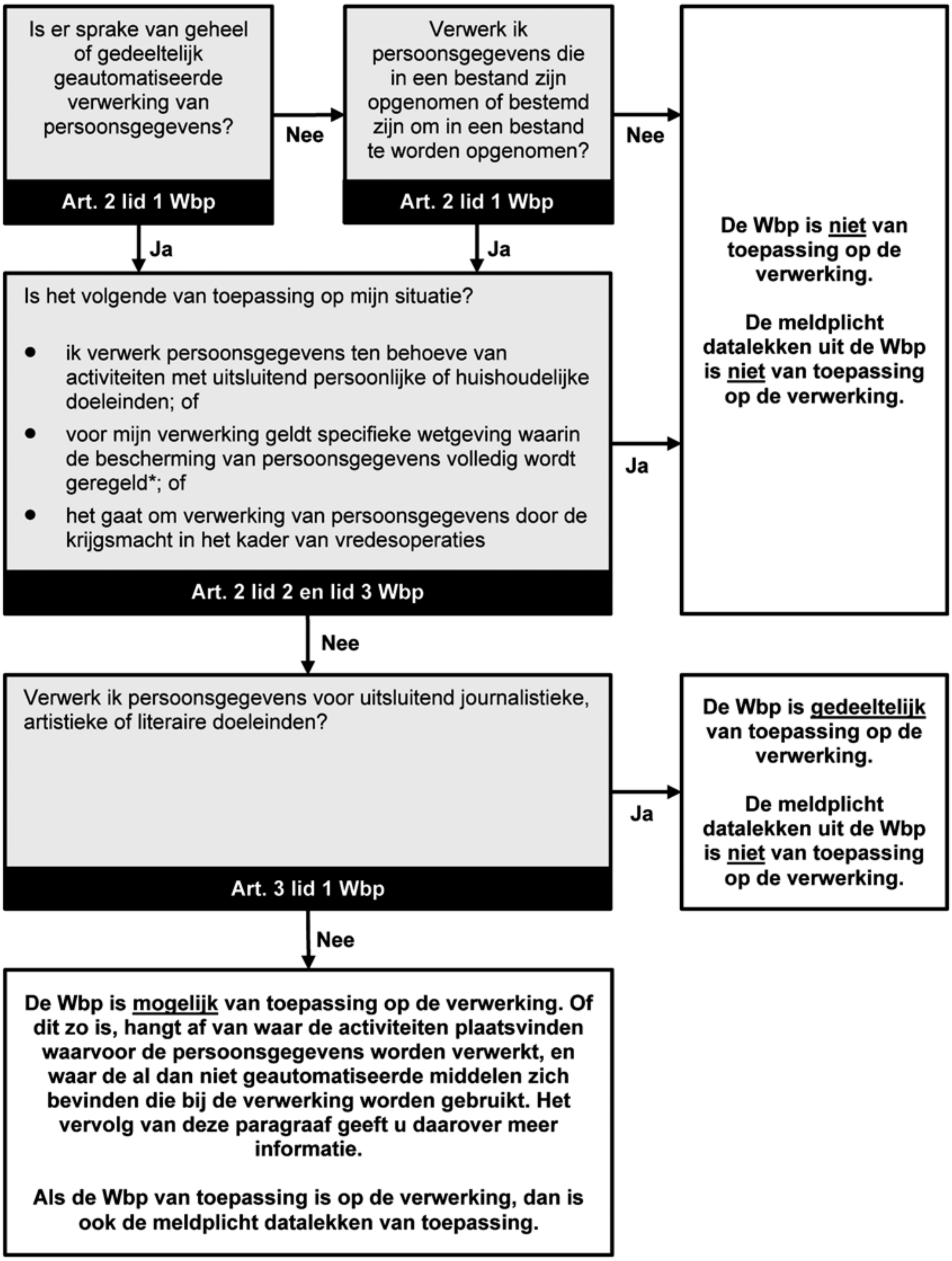
Voor de vraag of de Wbp van toepassing is op een verwerking van persoonsgegevens, zijn twee elementen van belang. Ten eerste moet u kijken naar de aard en de doelstelling van de verwerking. Bepaalde verwerkingen vallen door hun aard of hun doelstelling buiten de reikwijdte van de Wbp en op deze verwerkingen is de meldplicht datalekken niet van toepassing. Ten tweede is het van belang waar de activiteiten plaatsvinden waarvoor de persoonsgegevens worden verwerkt, en waar de al dan niet geautomatiseerde middelen zich bevinden die bij de verwerking worden gebruikt. Mogelijk is de privacywetgeving van een ander Europees land van toepassing op de verwerking of valt de verwerking niet onder de Europese privacywetgeving. Ook in deze situaties is de meldplicht datalekken uit de Wbp niet van toepassing.

De twee schema's in het vervolg van deze paragraaf lichten het bovenstaande nader toe. In beide schema's vindt u per onderdeel een verwijzing naar het relevante artikel uit de Wbp. Meer informatie over deze artikelen treft u aan in de Wbp-naslag op de website van de Autoriteit Persoonsgegevens.[6]

Het onderstaande schema geeft een leidraad voor het eerste element: de beoordeling op basis van de aard en de doelstelling van de verwerking.

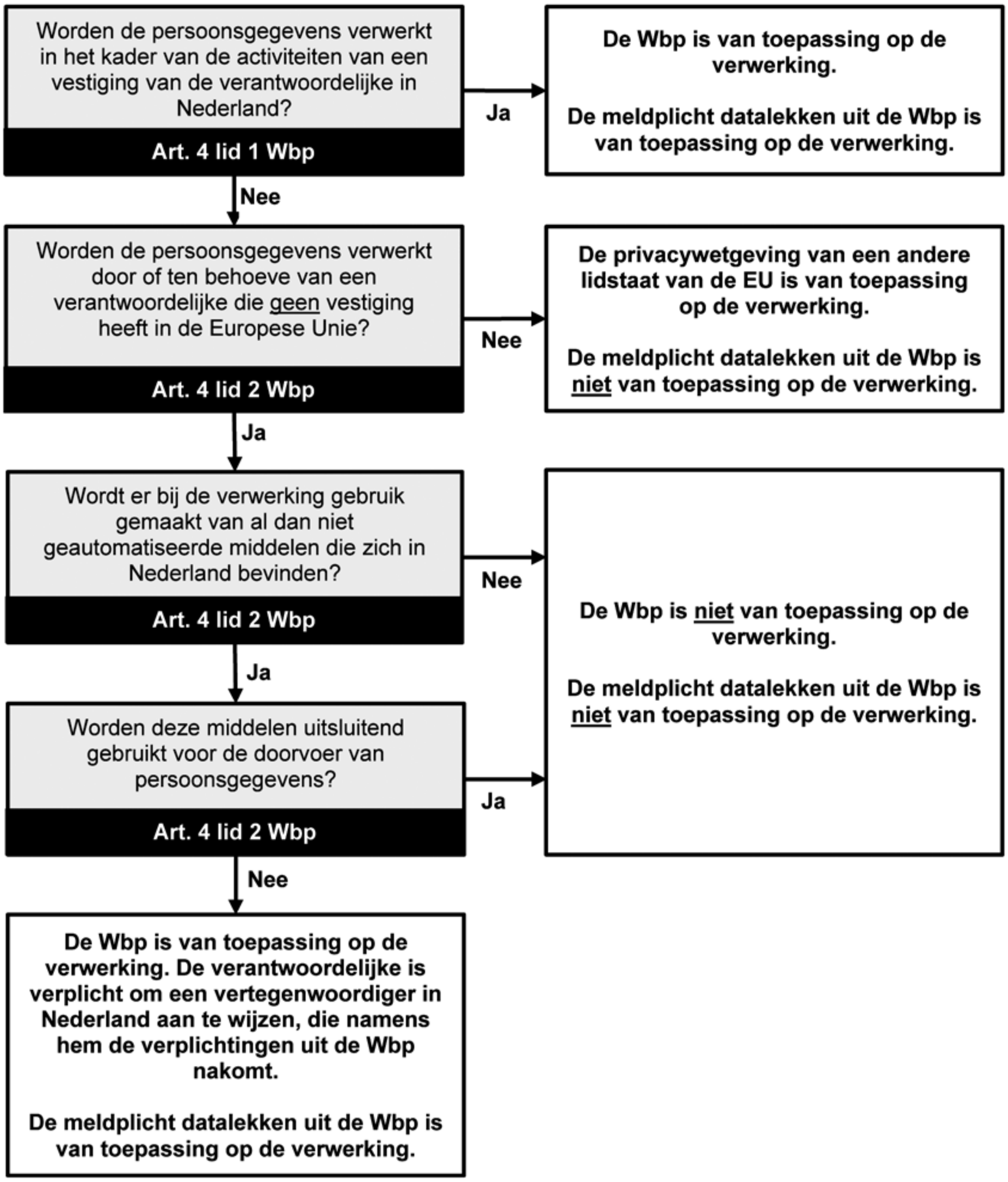
---

6 autoriteitpersoonsgegevens.nl.




*) Het tweede lid van artikel 2 Wbp bevat een volledige opsomming van deze wetgeving.

Voor verwerkingen die niet onder de hierboven weergegeven uitzonderingen vallen, is verder van belang waar de activiteiten plaatsvinden waarvoor de persoonsgegevens worden verwerkt, en waar de al dan niet geautomatiseerde middelen zich bevinden die bij de verwerking worden gebruikt. Het onderstaande schema licht dit nader toe.




**Voorbeeld meldplicht datalekken niet van toepassing op verwerking in Nederland**[7]
Een organisatie die in Frankrijk is gevestigd en die geen vestiging in Nederland heeft, laat persoonsgegevens bewerken door een bedrijf in Nederland. Aangezien de verantwoordelijke voor de verwerking in een ander Europees land is gevestigd, is de Wbp niet van toepassing op de verwerking en hoeft een eventueel datalek niet te worden gemeld aan de Autoriteit Persoonsgegevens.

## 2. Wat moet ik regelen als ik persoonsgegevens laat verwerken door een bewerker?

Veel verantwoordelijken laten de verwerking van hun persoonsgegevens geheel of gedeeltelijk uitvoeren door een zogeheten bewerker. Een bewerker verwerkt persoonsgegevens ten behoeve van de verantwoordelijke, zonder dat hij aan het rechtstreekse gezag van de verantwoordelijke is onderworpen (artikel 1, sub e, Wbp). Van verwerking door een bewerker is bijvoorbeeld sprake bij het verwerken van persoonsgegevens in de cloud of bij externe hosting van een website waar persoonsgegevens worden verwerkt. Dit hoofdstuk geeft antwoord op de vraag wat u moet regelen als de meldplicht datalekken uit de Wbp op u van toepassing is, en u bij de verwerking een bewerker

[7] Kamerstukken II, 2013/14, nr. 6, blz. 15.

inschakelt. Mocht u nog niet weten of de meldplicht datalekken op u van toepassing is, doorloop dan eerst de vragen uit hoofdstuk 1.

### *2.1. Waarom is het belangrijk om dit goed te regelen?*

Als u persoonsgegevens laat verwerken door een bewerker, dan moet u ervoor zorgen dat deze voldoende waarborgen biedt ten aanzien van de naleving van de meldplicht voor datalekken. U moet toezien op de naleving (artikel 14, eerste lid, Wbp).

U zorgt ervoor dat de bewerker de maatregelen treft die nodig zijn zodat u aan de meldplicht voor datalekken kunt voldoen (artikel 14, derde lid, sub c, Wbp).

In veel gevallen is de bewerker de eerste die kennis krijgt van een opgetreden datalek. Uw zorgplicht, als verantwoordelijke voor de verwerking, strekt zich expliciet uit over datalekken waarvan een bewerker kennis krijgt. Dat betekent dat u ervoor moet zorgen dat u, ook als u persoonsgegevens laat bewerken door een bewerker, in staat bent om uw wettelijke verplichtingen na te komen. In ieder geval moet u zorgen dat de bewerker u tijdig en adequaat informeert over de datalekken waarvan hij kennis krijgt.

Indien de concrete situatie zich daartoe leent, dan kunt u met de bewerker overeenkomen dat hij in het geval van een datalek de eerste melding aan de Autoriteit Persoonsgegevens doet. Voorwaarde is wel dat de bewerker, op basis van de afspraken die u met hem maakt, kan overzien in welke gevallen een melding aan de Autoriteit Persoonsgegevens noodzakelijk is. Als verantwoordelijke blijft u ook in dit geval eindverantwoordelijk voor de melding. Dit betekent dat u moet zorgen dat de bewerker u op de hoogte houdt als hij een datalek meldt aan de Autoriteit Persoonsgegevens.

### *2.2. Waarover moet ik afspraken maken met de bewerker?*

Afgezien van het toezien op naleving door de bewerker, dat in de voorgaande paragraaf werd aangehaald, schrijft de wet niet voor wat u precies met de bewerker af moet spreken. U moet in ieder geval denken aan het volgende:

- Gaat de bewerker u daadwerkelijk informeren over alle relevante incidenten?
- Gaat de bewerker eventueel zelf meldingen doen aan de Autoriteit Persoonsgegevens?
- Ontvangt u per incident alle informatie die u nodig heeft?
- Hoe gaat de bewerker u informeren over de incidenten?
- Wordt u tijdig geïnformeerd over de incidenten?
- Wordt u op de hoogte gehouden van eventuele nieuwe ontwikkelingen rond het incident, en van de maatregelen die de bewerker treft om aan zijn kant de gevolgen van het incident te beperken en herhaling te voorkomen?
- Kunt u vaststellen dat u daadwerkelijk op de hoogte wordt gesteld van alle relevante incidenten, en dat de verstrekte informatie klopt?

De Wbp verplicht u om te zorgen voor voldoende beveiliging van de persoonsgegevens die u verwerkt, ook als u bij de verwerking een bewerker inschakelt. Adequate beveiliging door de bewerker is in meerdere opzichten van belang voor de naleving van de meldplicht datalekken. Ten eerste levert een adequate beveiliging een belangrijke bijdrage aan het voorkomen van datalekken. Ten tweede stellen maatregelen zoals *intrusion detection* de bewerker in staat om (mogelijk) ongeoorloofde toegang tot persoonsgegevens tijdig te onderkennen en u daarover te informeren. Meer informatie over de beveiliging van persoonsgegevens bij verwerking door een bewerker treft u aan in de richtsnoeren *Beveiliging van persoonsgegevens* van de Autoriteit Persoonsgegevens.[8]

Hoewel u als verantwoordelijke verantwoordelijk en aansprakelijk bent voor de gegevensverwerking door de bewerker (zie artikel 12 Wbp), is ook de bewerker drager van rechten en plichten. Hij dient niet alleen de instructies van de verantwoordelijke op te volgen maar is eveneens zelfstandig aansprakelijk voor de naleving van de beginselen met betrekking tot de verwerking van persoonsgegevens die zijn opgenomen in hoofdstuk 1 en 2 van de Wbp.[9]

### *2.3. Hoe moet ik de afspraken vastleggen die ik met de bewerker maak?*

De afspraken die u hierover met de bewerker maakt legt u schriftelijk vast, of in een andere, gelijk-

8 autoriteitpersoonsgegevens.nl.
9 Kamerstukken II, 1997/98, 25 892, nr. 3, blz. 61. Zie ook: CBP, Onderzoek naar de beveiliging van Humannet Starter en Humannet Verzuim door VCD Humannet B.V., z2012-00288, Rapport definitieve bevindingen van december 2014.

waardige vorm (artikel 14, vijfde lid, Wbp). Een mondelinge afspraak tussen u als verantwoordelijke en de bewerker is niet voldoende.

### *2.4. Wat als ik gebruik maak van een bewerker in het buitenland?*

De vestigingsplaats van de bewerker is voor de meldplicht datalekken niet relevant. Ook datalekken die plaatsvinden bij een buitenlandse bewerker (die gevestigd is in een andere EU-lidstaat of in een land buiten de EU) moeten worden gemeld aan de Autoriteit Persoonsgegevens. Hiervoor geldt datgene dat in de voorafgaande paragrafen is aangegeven.

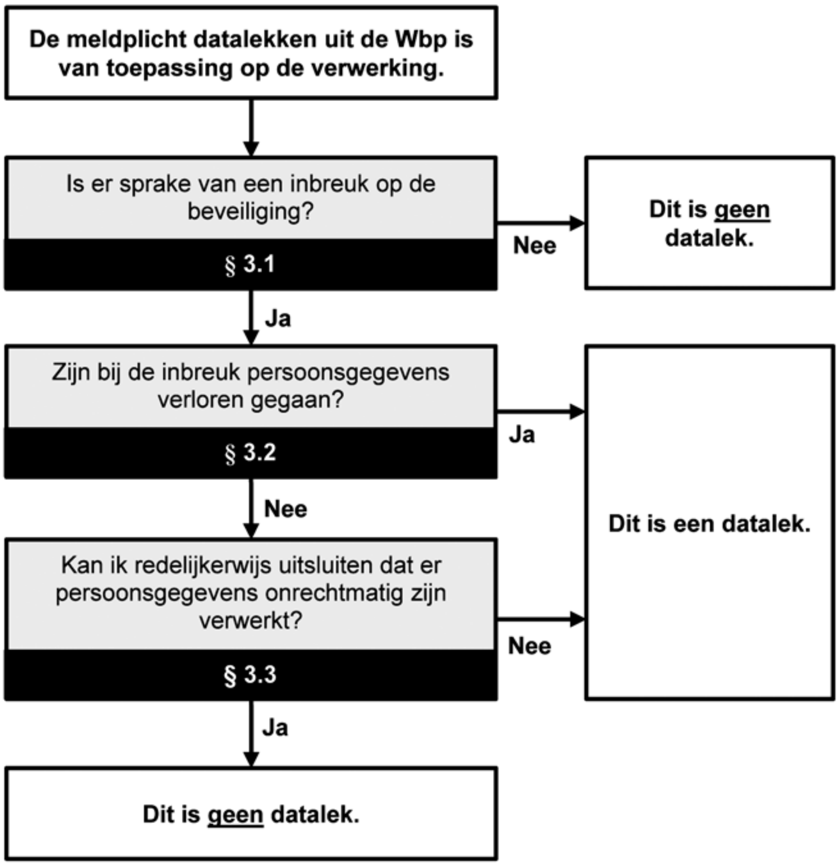
**Voorbeeld meldplicht datalekken van toepassing op verwerking in het buitenland**[10]
Een organisatie die in Nederland is gevestigd, laat persoonsgegevens bewerken door een bedrijf in Frankrijk. De persoonsgegevens bevinden zich op een server in Frankrijk. Als onbevoegden zich toegang verschaffen tot deze gegevens, dan valt dit onder de meldplicht datalekken onder de Wbp en dan moet dit door de Nederlandse verantwoordelijke worden gemeld aan de Autoriteit Persoonsgegevens.

Overigens schrijft het vierde lid van artikel 14 van de Wbp voor dat u, wanneer de bewerker gevestigd is in een andere lidstaat van de EU, er zorg voor moet dragen dat de bewerker het recht van die lidstaat nakomt. Het 'recht van die lidstaat' heeft betrekking op de lokale verplichtingen op het gebied van informatiebeveiliging. Dit betekent dat u in de bewerkersovereenkomst de naleving moet waarborgen van de beveiligingsmaatregelen zoals die zijn gedefinieerd door de wetgeving van de lidstaat waarin de verwerker is gevestigd.[11]

## 3. Is dit een datalek?

Het eerste lid van artikel 34a, Wbp spreekt over een "een inbreuk op de beveiliging, bedoeld in artikel 13". Kortheidshalve wordt een dergelijke inbreuk in deze beleidsregels aangeduid als een datalek. Dit hoofdstuk helpt u om vast te stellen of u een gebeurtenis die zich heeft voorgedaan moet beschouwen als een datalek. Uitgangspunt is dat de meldplicht datalekken uit de Wbp van toepassing is op de verwerking waarover het gaat. Mocht u nog niet weten of dat het geval is, doorloop dan eerst de vragen uit hoofdstuk 1.

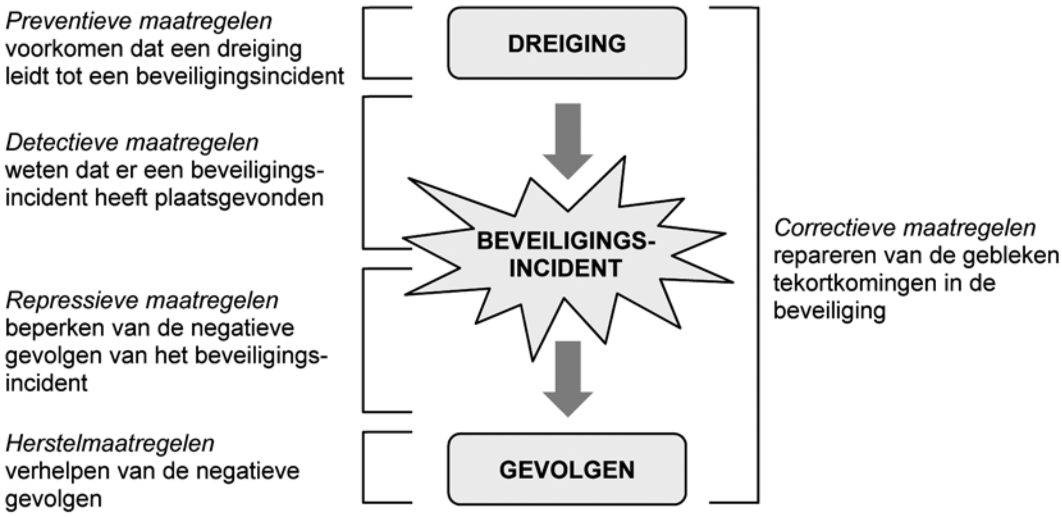
[10] Kamerstukken II, 2013/14, nr. 6, blz. 16.
[11] Zie ook: Artikel 29-Werkgroep, Advies 8/2018 over toepasselijk recht, paragraaf III.5.




### *3.1 Is er sprake van een inbreuk op de beveiliging?*

Artikel 13 Wbp verplicht u als verantwoordelijke om passende technische en organisatorische maatregelen ten uitvoer te leggen om persoonsgegevens te beveiligen tegen verlies of enige vorm van onrechtmatige verwerking.

De maatregelen waarop wordt gedoeld in artikel 13 Wbp zijn onder te verdelen in een aantal typen. Deze vindt u terug in het onderstaande schema. Het vervolg van deze paragraaf licht aan de hand van dit schema nader toe in welke gevallen er sprake is van een inbreuk op de beveiliging.




Een inbreuk op de beveiliging houdt in dat zich daadwerkelijk een beveiligingsincident heeft voorgedaan. Er is niet uitsluitend sprake van een dreiging, of van een tekortkoming in de beveiliging (ook wel aangeduid als een beveiligingslek) die zou kunnen leiden tot een beveiligingsincident. Er heeft zich daadwerkelijk een beveiligingsincident voorgedaan, en de preventieve maatregelen die u eventueel

heeft getroffen waren niet toereikend om dit te voorkomen.

Bij beveiligingsincidenten waar sprake kan zijn van een inbreuk op de beveiliging van persoonsgegevens moet u bijvoorbeeld denken aan:
- een kwijtgeraakte USB-stick;
- een gestolen laptop;
- een inbraak door een hacker;
- een malware-besmetting;
- een calamiteit zoals een brand in een datacentrum.

Kenmerkend voor een inbreuk op de beveiliging is verder dat het beveiligingsincident daadwerkelijk gevolgen heeft voor de persoonsgegevens die u verwerkt. Er zijn persoonsgegevens verloren gegaan, of u kunt niet redelijkerwijs uitsluiten dat er persoonsgegevens onrechtmatig zijn verwerkt. De repressieve maatregelen en de herstelmaatregelen die u eventueel heeft getroffen waren niet voldoende om deze gevolgen geheel weg te nemen.

Een inbreuk op de beveiliging van persoonsgegevens moet ruim worden geduid. Het is niet van belang of u passende technische of organisatorische maatregelen heeft getroffen of niet. Een datalek kan zich in beide situaties voordoen.[12]

### *3.2 Zijn bij de inbreuk persoonsgegevens verloren gegaan?*

Verlies houdt in dat u de persoonsgegevens niet meer heeft. Bij het beveiligingsincident zijn de persoonsgegevens vernietigd of op een andere manier verloren gegaan, en u beschikt niet over een complete en actuele reservekopie van de gegevens. In deze situatie is er sprake van een datalek.

**Voorbeeld wel / geen datalek (verlies van persoonsgegevens)**
Een database met persoonsgegevens is vernietigd als gevolg van een menselijke fout van een systeembeheerder. Van de database is een complete, actuele back-up beschikbaar, op basis waarvan de database direct weer wordt opgebouwd. In deze situatie is er geen sprake van een datalek.

De aard van het beveiligingsincident is niet relevant voor de vraag of er al dan niet sprake is van een datalek. Anders dan de memorie van toelichting bij de wetswijziging suggereert,[13] is er ook sprake van een datalek als de persoonsgegevens verloren zijn gegaan als gevolg van een calamiteit en er geen actuele reservekopie beschikbaar is.

### *3.3 Kan ik redelijkerwijs uitsluiten dat er persoonsgegevens onrechtmatig zijn verwerkt?*

Onder onrechtmatige vormen van verwerking vallen de aantasting van de persoonsgegevens, onbevoegde kennisneming, wijziging, of verstrekking daarvan. Als u redelijkerwijs niet kunt uitsluiten dat een inbreuk op de beveiliging tot een onrechtmatige verwerking heeft geleid, dan moet u de inbreuk beschouwen als een datalek.[14]

**Voorbeeld wel / geen datalek (onrechtmatige verwerking van persoonsgegevens)**[15]
Een werknemer geeft aan een derde de gebruikersnaam en het wachtwoord die toegang geven tot alle klantgegevens van alle klanten van het bedrijf waar hij werkt.
Na ontdekking van het gebeurde past het bedrijf het wachtwoord van het betreffende account aan, zodat de derde geen toegang meer heeft.
Daarna onderzoekt het bedrijf of de derde daadwerkelijk toegang heeft gezocht tot de klantgegevens. Bij dit onderzoek maakt het bedrijf gebruik van logbestanden, waarin per gebruikersnaam is vastgelegd welke acties er op welk tijdstip zijn uitgevoerd met welke klantgegevens.
Als op basis van de logbestanden redelijkerwijs kan worden uitgesloten dat er door middel van het betreffende account toegang is verkregen tot de klantgegevens, dan is er uitsluitend sprake van een beveiligingslek en niet van een datalek.

Bij een malware-besmetting moet u ervan uitgaan dat er sprake kan zijn van een datalek. Bepaalde typen malware doorzoeken de besmette apparatuur op waardevolle persoonsgegevens zoals e-mailadressen, gebruikersnamen en wachtwoorden en creditcardgegevens, om de gevonden gegevens vervolgens weg te sluizen naar een server die in handen is van de aanvaller. Een dergelijke

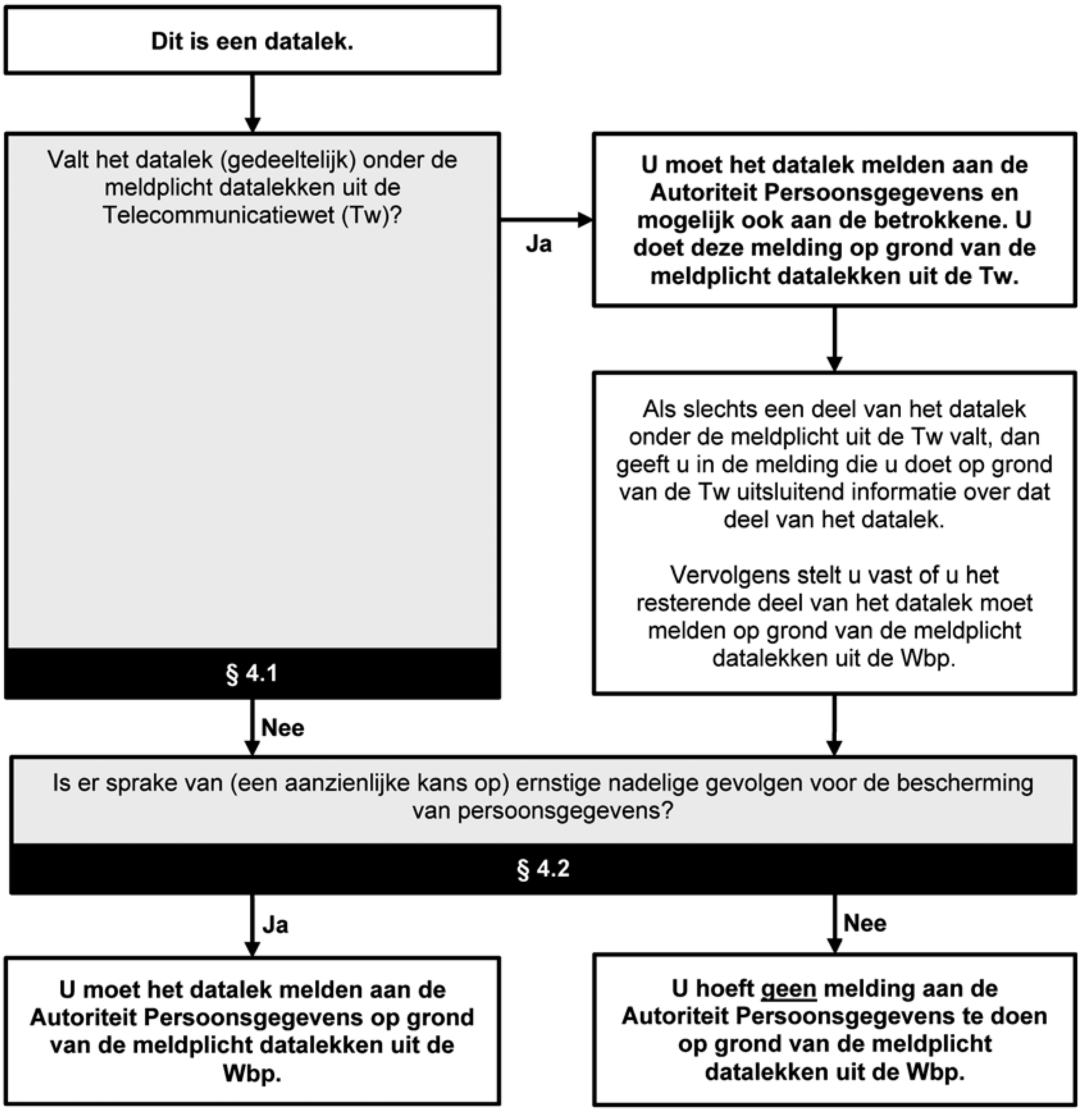
---

[12] Kamerstukken II 2013/14, 33 662, nr. 6, blz. 4.
[13] Kamerstukken II 2012/13 33 662, nr. 3, blz. 5–6.
[14] Kamerstukken II 2014/15, 33 662, nr. 11, blz. 4.
[15] Bron: Artikel 29-Werkgroep, Advies 03/2014 over kennisgeving bij inbreuken in verband met persoonsgegevens, goedgekeurd op 25 maart 2014, Casus 3.

malware-besmetting stelt de getroffen persoonsgegevens dus bloot aan onbevoegde kennisname en andere vormen van onrechtmatige verwerking. Andere typen malware maken bestanden ontoegankelijk voor de rechtmatige eigenaar door ze te blokkeren ('ransomware') of te versleutelen ('cryptoware'). Door deze vormen van malware worden de getroffen persoonsgegevens dus blootgesteld aan onbevoegde aantasting of wijziging.

### 4. Moet ik dit datalek melden aan de Autoriteit Persoonsgegevens?

Het onderstaande schema geeft de vragen weer die u moet beantwoorden om vast te stellen of u een specifiek datalek moet melden aan de Autoriteit Persoonsgegevens. Iedere vraag uit het onderstaande schema correspondeert met een paragraaf uit het vervolg van dit hoofdstuk. Uitgangspunt is dat er een gebeurtenis heeft plaatsgevonden waarvan u al heeft vastgesteld dat het gaat om een datalek. Mocht u dit nog niet hebben vastgesteld, doorloop dan eerst de vragen uit hoofdstuk 3.




#### *4.1. Valt het datalek (gedeeltelijk) onder de meldplicht datalekken uit de Tw?*

Als u een aanbieder van een openbare elektronische communicatiedienst bent, dan heeft u te maken met twee meldplichten voor datalekken: de al langer bestaande meldplicht in de Tw en de meldplicht datalekken in de Wbp.

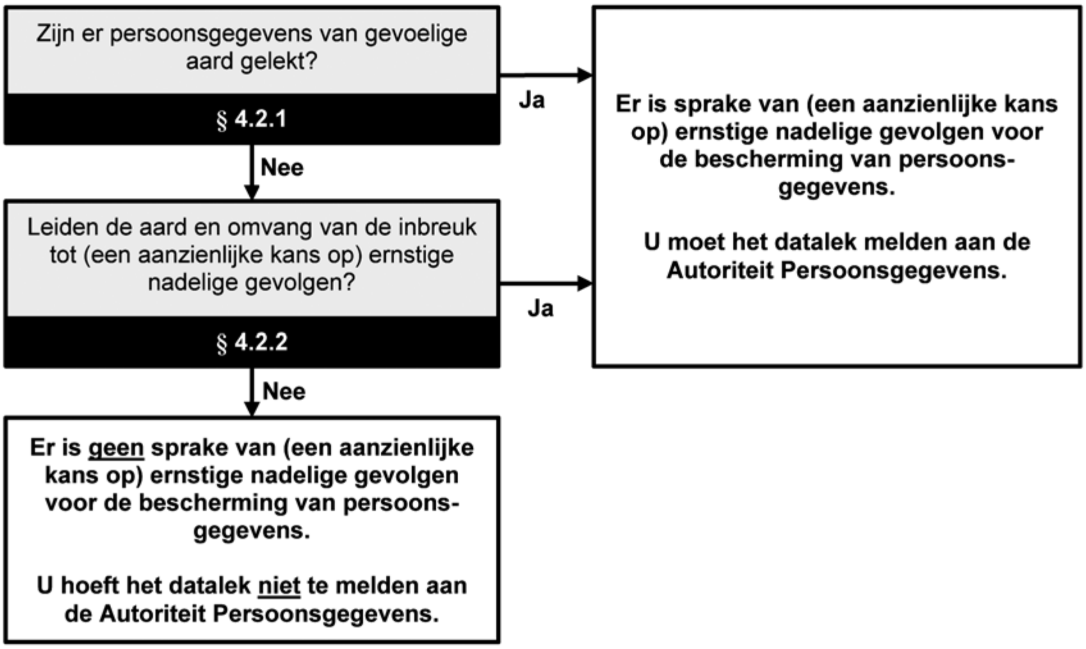
Het uitgangspunt is dat u een datalek dat onder de meldplicht uit de Tw valt, niet (nogmaals) hoeft te melden op grond van de Wbp (artikel 34a, negende lid, Wbp).

Het kan zijn dat een datalek gedeeltelijk betrekking heeft op persoonsgegevens die onder de meldplicht in de Tw vallen, maar deels ook op persoonsgegevens die daarbuiten vallen. Een voorbeeld van een dergelijke situatie is de diefstal van een laptop waarop zowel klantgegevens als personeelsgegevens staan. De diefstal van de klantgegevens valt onder de meldplicht uit de Tw en de diefstal van de personeelsgegevens valt onder de meldplicht datalekken uit de Wbp. Het is mogelijk dat u in een dergelijk geval twee meldingen moet doen, een op grond van de meldplicht in de Tw en een op grond van de meldplicht datalekken in de Wbp.

### *4.2. Is er sprake van (een aanzienlijke kans op) ernstige nadelige gevolgen voor de bescherming van persoonsgegevens?*

Er is sprake van een geclausuleerde meldplicht voor datalekken. Dat wil zeggen dat u een inbreuk alleen hoeft te melden als deze leidt tot een aanzienlijke kans op ernstige nadelige gevolgen dan wel ernstige nadelige gevolgen heeft voor de bescherming van persoonsgegevens (artikel 34a, eerste lid, Wbp).

Het is aan u om te bepalen of een datalek dat u binnen uw organisatie heeft ontdekt binnen de reikwijdte van de meldplicht datalekken aan de Autoriteit Persoonsgegevens valt. Doel van de rest van deze paragraaf is om deze afweging te ondersteunen.[16]




Iedere vraag uit het bovenstaande schema correspondeert met een van de onderstaande paragrafen. Voorafgaand daaraan, treft u onderstaand nog een aantal voorbeelden aan.

**Voorbeelden van datalekken die moeten worden gemeld aan de Autoriteit Persoonsgegevens (1)**[17]

- Intern wordt binnen een ziekenhuis gesignaleerd dat door een haperende beveiliging (technische storing) medische gegevens zijn ingezien door onbevoegden;
- Een journalistiek programma confronteert een bedrijf met het feit dat als gevolg van een beveiligingslek onder andere persoonlijke gegevens (zoals kopieën van paspoorten of rijbewijzen, bankgegevens en wachtwoorden) van werknemers op de server van het bedrijf door onbevoegden zijn ingezien;
- Een medewerker verliest een laptop met onversleutelde, financiële klantgegevens;
- Een bedrijf krijgt te maken met een hack waarbij klantgegevens en wachtwoorden zijn ontvreemd;
- Een overheidsdatabase met gevoelige persoonsgegevens wordt gehackt waardoor onbevoegden toegang hebben gekregen tot deze gegevens.

[16] Kamerstukken I 2014/15, 33 662, nr. C, blz. 17.
[17] Kamerstukken II 2014/15 33 662, nr. 11, blz. 11.

**Voorbeelden van datalekken die moeten worden gemeld aan de Autoriteit Persoonsgegevens (2)**[18]

1. Vier laptops zijn gestolen bij een gezondheidscentrum voor kinderen. De laptops bevatten gevoelige gegevens over gezondheid en welzijn en andere persoonsgegevens van meer dan 2000 kinderen.
2. Bij een levensverzekeraar zijn persoonsgegevens ongeoorloofd in te zien als gevolg van een kwetsbaarheid in een webapplicatie. Van 700 personen kunnen naam, adres en formulieren met medische gegevens worden ingezien.
3. Een medewerker van een internetprovider heeft zijn login/wachtwoordgegevens aan een derde partij gegeven die daardoor nagenoeg onbeperkt bij alle klantgegevens (meer dan 100.000) kon komen.
4. Een envelop met creditcardbetalingsgegevens van 800 personen was per ongeluk niet versnipperd, maar in een vuilnisbak gegooid. Een derde persoon haalde de gegevens uit de vuilniscontainer op straat en verstrekte ze aan andere personen.
5. De versleutelde laptop van een financieel adviseur is uit de auto gestolen. Financiële gegevens (hypotheken, salarissen, leningen) van 1000 personen waren betrokken. Hoewel het wachtwoord van de laptop niet gecompromitteerd is, was er geen back-up voorhanden.
6. Op de website van een telefoonbedrijf kunnen klanten inloggen en hun financiële gegevens en belgegevens inzien. Een derde partij heeft toegang gekregen tot de database met inlognamen en bijbehorende verhaspelde (onleesbaar gemaakte) wachtwoorden. Het is echter mogelijk dat bepaalde wachtwoorden achterhaald kunnen worden.
7. Een internetprovider biedt de gebruikers de mogelijkheid om details van hun account te zien, zoals onder andere historische zoekgegevens en vaak bezochte websites. Door een fout in de website had eenieder via een simpele truc de mogelijkheid om de accounts van andere gebruikers vrijelijk in te zien. Zonder een sluitende logging is hier niet vast te stellen of dat daadwerkelijk is gebeurd en welke gegevens dan zijn geraadpleegd.

Alle bovengenoemde voorbeelden zijn ontleend aan de parlementaire geschiedenis. De laatstgenoemde voorbeelden zijn oorspronkelijk afkomstig uit Advies 03/2014 van de Artikel 29-Werkgroep. In een aantal van deze voorbeelden worden grote aantallen betrokkenen genoemd. Echter: de meldplicht kan ook van toepassing zijn op een datalek dat slechts betrekking heeft op de gegevens van één persoon.

**Voorbeelden van gebeurtenissen die niet onder de meldplicht vallen**

- Een brief met daarin persoonsgegevens wordt naar een foutief adres gestuurd, en wordt ongeopend retour gezonden.
- Iemand laat een koffer met daarin persoonsgegevens achter in de trein. De koffer is voorzien van een deugdelijk slot, en komt via ‘gevonden voorwerpen’ ongeopend terug bij de rechtmatige eigenaar.
- Het zoekraken of hacken van de ledenadministratie van een sportvereniging zal doorgaans leiden tot het nodige ongemak voor verenging en leden, maar zal niet snel aanleiding geven tot een melding bij het CBP.[19] Dit kan overigens anders liggen als de sportvereniging zich bijvoorbeeld richt op personen met een specifieke levensovertuiging of seksuele geaardheid, of als er fraudegevoelige gegevens gelekt zijn.
- Als ziekenhuispersoneel gebruik maakt van het wachtwoord van een arts om toegang te krijgen tot medische persoonsgegevens, dan is er niet zo zeer sprake van een datalek, als van schending van interne voorschriften. In eerste instantie liggen dan disciplinaire maatregelen voor de hand.[20]

### *4.2.1. Zijn er persoonsgegevens van gevoelige aard gelekt?*

Bij het beantwoorden van de vraag of er sprake is van (een aanzienlijke kans op) ernstige nadelige gevolgen voor de bescherming van de verwerkte persoonsgegevens, moet u in ieder geval kijken naar de aard van de getroffen gegevens. Is er sprake van bijzondere persoonsgegevens of van persoonsgegevens die anderszins van gevoelige aard zijn?[21] Bij dit laatste moet u bijvoorbeeld denken aan gegevens over betalingsachterstanden.[22]

Bij een aantal categorieën van persoonsgegevens, in dit kader aangeduid als persoonsgegevens van

[18] Volledigheidshalve zijn hier ook de voorbeelden opgenomen die betrekking hebben op de telecomsector. De voorbeelden worden aangehaald in Kamerstukken I 2014/15, 33 662, nr. C, blz. 24, en zijn ontleend aan Advies 03/2014 over kennisgeving bij inbreuken in verband met persoonsgegevens, goedgekeurd op 25 maart 2014, van de Artikel 29-Werkgroep. Bij de geciteerde voorbeelden is aangegeven dat het bij de voorbeelden 1 tot en met 5 gaat om inbreuken met nadelige gevolgen, en bij de voorbeelden 6 en 7 om inbreuken met een aanzienlijke kans op nadelige gevolgen.
[19] Kamerstukken II 2012/13, 33 662, nr. 3, blz. 7.
[20] Handelingen II 2014/15 nr. 51, item 9, blz. 32.
[21] Kamerstukken II 2013/14, 33 662, nr. 6, blz. 19.
[22] Handelingen II 2014/15, nr. 51, item 9, blz. 24.

gevoelige aard, kunnen verlies of onrechtmatige verwerking onder meer leiden tot stigmatisering of uitsluiting van de betrokkene, tot schade aan de gezondheid, financiële schade of tot (identiteits-)fraude. Tot deze categorieën van persoonsgegevens moeten in ieder geval worden gerekend:

- *Bijzondere persoonsgegevens zoals bedoeld in artikel 16 Wbp*
  Het gaat hierbij om persoonsgegevens over iemands godsdienst of levensovertuiging, ras, politieke gezindheid, gezondheid, seksuele leven, lidmaatschap van een vakvereniging en om strafrechtelijke persoonsgegevens en persoonsgegevens over onrechtmatig of hinderlijk gedrag in verband met een opgelegd verbod naar aanleiding van dat gedrag.
- *Gegevens over de financiële of economische situatie van de betrokkene*
  Hieronder vallen bijvoorbeeld gegevens over (problematische) schulden, salaris- en betalingsgegevens.
- *(Andere) gegevens die kunnen leiden tot stigmatisering of uitsluiting van de betrokkene*
  Hieronder vallen bijvoorbeeld gegevens over gokverslaving, prestaties op school of werk of relatieproblemen.
- *Gebruikersnamen, wachtwoorden en andere inloggegevens*
  De mogelijke gevolgen voor betrokkenen hangen af van de verwerkingen en van de persoonsgegevens waar de inloggegevens toegang toe geven. Bij de afweging moet worden betrokken dat veel mensen wachtwoorden hergebruiken voor verschillende verwerkingen.
- *Gegevens die kunnen worden misbruikt voor (identiteits)fraude*
  Het gaat hierbij onder meer om biometrische gegevens, kopieën van identiteitsbewijzen en om het Burgerservicenummer (bsn).

Ook gegevens uit DNA-databanken, gegevens waar een bijzondere, wettelijk bepaalde geheimhoudingsplicht op rust en gegevens die onder een beroepsgeheim vallen (bijvoorbeeld het medisch beroepsgeheim) in de zin van artikel 9, vierde lid, van de Wbp moeten tot de persoonsgegevens van gevoelige aard worden gerekend.

**Voorbeeld persoonsgegevens van gevoelige aard bij hack**
Een hacker weet op de website van een lokale sportvereniging door middel van SQL-injectie, een veel voorkomende vorm van hacking, een bestand te bemachtigen met daarin de namen en e-mailadressen van een twintigtal abonnees op een nieuwsbrief.
Normaal gesproken gaat het hier niet om persoonsgegevens van gevoelige aard. Dit wordt anders als de sportvereniging of de nieuwsbrief zich richt op mensen met, bijvoorbeeld, een specifieke levensovertuiging, politieke voorkeur of seksuele geaardheid.

### *4.2.2. Leiden de aard en omvang van de inbreuk tot (een aanzienlijke kans op) ernstige nadelige gevolgen?*

De memorie van toelichting geeft aan dat de aard en omvang van de getroffen verwerking mede bepalend zijn voor de beantwoording van de vraag of er bij een datalek sprake is van (een aanzienlijke kans op) nadelige gevolgen voor de bescherming van persoonsgegevens. Een datalek bij instellingen als de Belastingdienst, de Sociale Verzekeringsbank (SVB) of bij een commerciële bank of verzekeraar kan leiden tot financieel nadeel voor de betrokkene of tot de compromittering van gegevens die beschermd worden door een geheimhoudingsplicht.[23] Beveiligingslekken in de omvangrijke verwerkingen van persoonsgegevens waarover de overheid beschikt kunnen ook zeer grote gevolgen hebben voor de betrokkenen.[24]

Afgezien van de gevoelige aard van de verwerkte gegevens, die in de voorgaande paragraaf al aan de orde kwam, is voor de kans op ernstige nadelige gevolgen voor de bescherming van de verwerkte persoonsgegevens verder het volgende relevant:

- De omvang van de hierboven beschreven verwerkingen betekent dat het bij datalekken kan gaan om veel persoonsgegevens per persoon, en om gegevens van grote groepen betrokkenen. Deze beide factoren maken een gelekte dataset aantrekkelijk voor misbruik in het criminele circuit. De kans dat de gelekte dataset wordt doorverkocht wordt daardoor ook groter, met als gevolg dat de betrokkenen langer last houden van het datalek.
- Naarmate de beslissingen die op basis van de verwerkte persoonsgegevens worden genomen ingrijpender zijn, is ook de impact van verlies of onrechtmatige verwerking groter. Bijvoorbeeld: als een organisatie financiële gegevens gebruikt om iemands kredietwaardigheid te bepalen zijn de gevolgen van verlies en onbevoegde wijziging van de gegevens ingrijpender dan bij gebruik van dezelfde gegevens voor marketingdoeleinden.
- Bij omvangrijke verwerkingen van de overheid is vaak sprake van persoonsgegevens die binnen ketens worden gedeeld. Dit betekent dat de gevolgen van verlies en onbevoegde wijziging van

[23] Kamerstukken II 2012/13, 33 662, nr. 3, blz. 7.
[24] Kamerstukken II 2012/13, 33 662, nr. 3, blz. 20.

persoonsgegevens door de hele keten heen kunnen optreden. Voor de betrokkenen wordt het hierdoor moeilijker om de mogelijke gevolgen van een datalek te overzien en om zich daar waar mogelijk aan te onttrekken.

Als de aard en omvang van de getroffen verwerking voldoen aan het bovenstaande, dan moet u ervan uitgaan dat er (een aanzienlijke kans op) ernstige nadelige gevolgen voor de bescherming van de verwerkte persoonsgegevens aanwezig kan zijn.

Behalve voor de aard en de omvang van de getroffen verwerking, wordt in de parlementaire geschiedenis ook aandacht gevraagd voor de positie van kwetsbare groepen.[25] Voor betrokkenen in kwetsbare groepen kan verlies of onrechtmatige verwerking van persoonsgegevens extra risico's met zich meebrengen. De gevolgen van onbevoegde toegang tot NAW-gegevens zullen bijvoorbeeld voor de meeste mensen beperkt zijn, maar dit ligt anders voor mensen die te maken hebben met stalking of die in een blijf-van-mijn-lijfhuis verblijven. Voor bepaalde categorieën van betrokkenen, zoals kinderen en mensen met een verstandelijke handicap, kan het moeilijker zijn om adequaat om te gaan met de gevolgen van een datalek. Zo zullen zij mogelijk eerder ingaan op pogingen tot phishing of oplichting.

Als u weet dat u gegevens verwerkt van mensen in kwetsbare groepen, bijvoorbeeld omdat de verwerking zich specifiek richt op betrokkenen die hiertoe behoren, dan moet u ervan uitgaan dat bij een datalek (een aanzienlijke kans op) ernstige nadelige gevolgen voor de bescherming van de verwerkte persoonsgegevens aanwezig kan zijn.

**Voorbeeld kwetsbare groepen**
Een hacker weet op de website van een buurthuis door middel van SQL-injectie, een veel voorkomende vorm van hacking, een bestand te bemachtigen met daarin de namen en e-mailadressen van een twintigtal abonnees op een elektronische nieuwsbrief. De nieuwsbrief richt zich op buurtbewoners van 65 jaar en ouder die bij het buurthuis een cursus volgen om vertrouwd te raken met het gebruik van computers en het internet. De aard van de doelgroep leidt hier tot extra risico's voor de betrokkenen. Gezien de onervarenheid van de betrokkenen met digitale communicatie bestaat er een aanzienlijk risico dat zij in zullen gaan op pogingen tot phishing of oplichting.

Bij een datalek als gevolg van een (niet-ethische) hack (art. 138ab van het Wetboek van Strafrecht), is van belang wat de aard van de gelekte persoonsgegevens is, en wat de risico's van misbruik van deze persoonsgegevens voor de betrokkene zijn. Bij een hack zal melding al snel gepast zijn gelet op de risico's van misbruik van persoonsgegevens. Bij een hack ligt ook aangifte bij de politie in de rede in verband met opsporing van de daders.[26]

### 5. Hoe moet ik het datalek melden aan de Autoriteit Persoonsgegevens?

De Autoriteit Persoonsgegevens stelt een webformulier beschikbaar waarmee datalekken kunnen worden gemeld.[27] Een overzicht van de vragen in dit webformulier treft u aan in een bijlage bij deze beleidsregels.

Als u geen gebruik kunt maken van het webformulier, dan kunt u de gevraagde gegevens per fax toezenden aan de Autoriteit Persoonsgegevens. U moet daarbij zorgen dat u aan kunt tonen dat u de melding tijdig heeft gedaan.

U ontvangt per omgaande een ontvangstbevestiging.

Bij die meldingen die aanleiding geven tot nadere actie door de Autoriteit Persoonsgegevens, zal deze contact met u opnemen om de herkomst van de melding te verifiëren. Op termijn zal worden aangesloten op eHerkenning of andere gangbare authenticatiemiddelen.

### 6. Wanneer moet ik het datalek melden aan de Autoriteit Persoonsgegevens?

U moet het datalek onverwijld melden aan de Autoriteit Persoonsgegevens (artikel 34a, eerste lid, Wbp).

Het onverwijld melden houdt in dat u, na het ontdekken van een mogelijk datalek, enige tijd mag nemen voor nader onderzoek teneinde een onnodige melding te voorkomen.

---

[25] Handelingen II 2014/15, nr. 51, item 9, blz.
[26] Kamerstukken II 2013/14, nr. 6, blz. 19.
[27] autoriteitpersoonsgegevens.nl.

Wat in een concreet geval als 'onverwijld' moet worden aangemerkt zal afhangen van de omstandigheden van het geval. Onderstaand treft u de uitgangspunten aan die de Autoriteit Persoonsgegevens met het oog op zijn toezichthoudende en handhavende bevoegdheden hanteert.[28]

De termijn voor het melden van het datalek begint te lopen op het moment dat uzelf, of een bewerker die u heeft ingeschakeld, op de hoogte raakt van een incident dat mogelijk onder de meldplicht datalekken valt.

Zonder onnodige vertraging, en zo mogelijk niet later dan 72 uur na de ontdekking, doet u een melding bij de Autoriteit Persoonsgegevens, tenzij op dat moment inmiddels al uit uw onderzoek is gebleken dat het incident niet onder de meldplicht datalekken valt. Indien u het incident later dan 72 uur na ontdekking aan de toezichthouder meldt, dan kunt u desgevraagd motiveren waarom u de melding later heeft gedaan.[29]

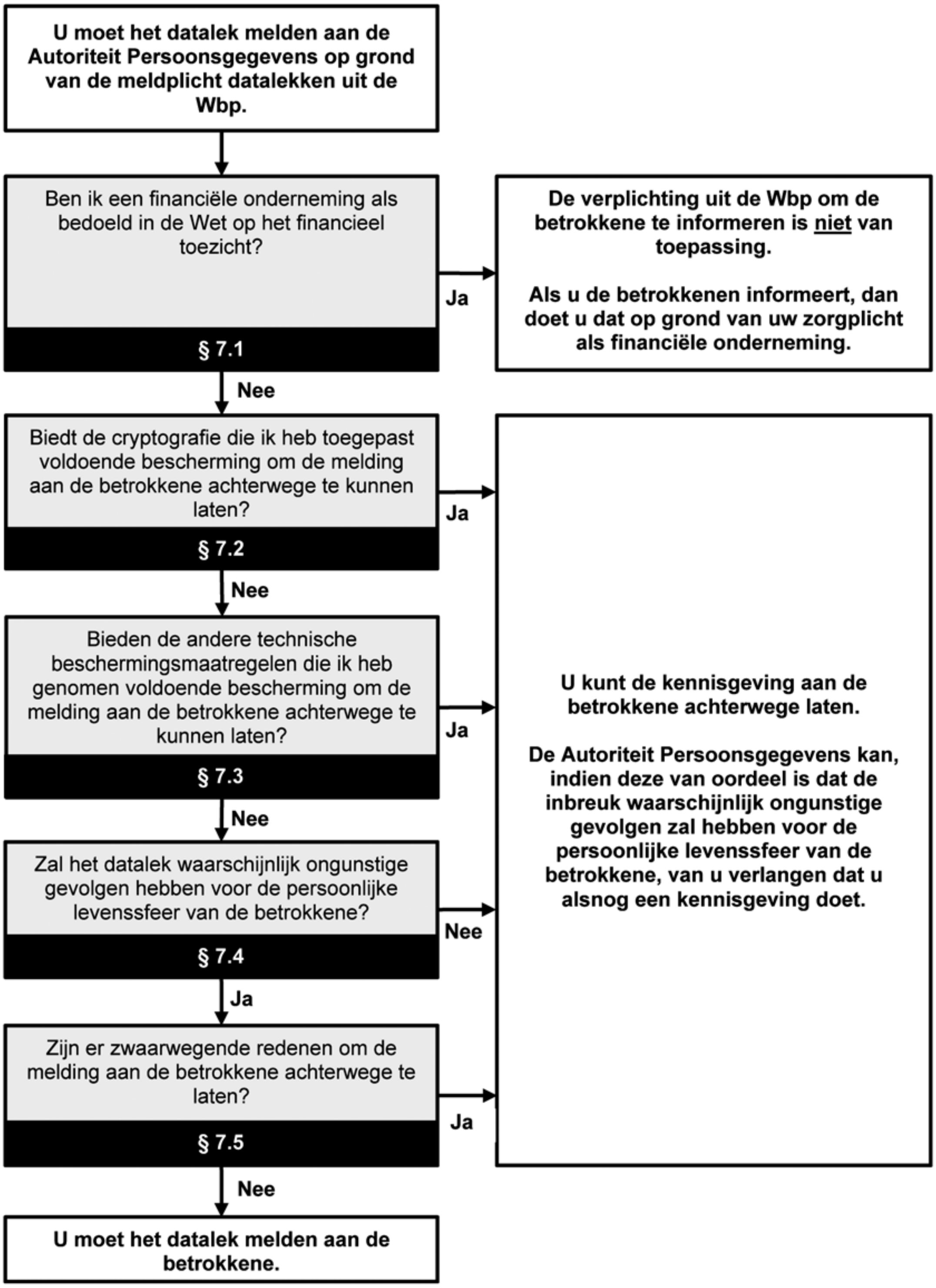
Mogelijk heeft u 72 uur na de ontdekking van het incident nog niet volledig zicht op wat er gebeurd is en om welke persoonsgegevens het gaat. In dat geval doet u de melding op basis van de gegevens waarover u op dat moment beschikt. Eventueel kunt u de melding naderhand nog aanvullen of intrekken.

Om datalekken tijdig te kunnen melden zult u goede afspraken moeten maken met de bewerkers die u eventueel inschakelt, zodat zij u tijdig en adequaat informeren over alle relevante incidenten.

### 7. Moet ik het datalek melden aan de betrokkene?

Het onderstaande schema geeft de vragen weer die u moet beantwoorden om vast te stellen of u een specifiek datalek moet melden aan de betrokkenen. Iedere vraag uit het schema correspondeert met een paragraaf uit het vervolg van dit hoofdstuk.

[28] Kamerstukken II 2013/14, 33 662, nr. 6, blz. 16.
[29] Zie art. 31, eerste lid, van de concept-Algemene Privacy-verordening, uit de tekst zoals geamendeerd door de Raad van de Europese Unie: "In geval van een inbreuk in verband met persoonsgegevens […] meldt de verantwoordelijke de overeenkomstig artikel 51 bevoegde toezichthoudende autoriteit deze inbreuk zonder onnodige vertraging en zo mogelijk niet later dan 72 uur nadat hij ervan kennis heeft gekregen. Wanneer de melding aan de toezichthoudende autoriteit niet binnen 72 uur plaatsvindt, gaat deze vergezeld van een motivering."




Uitgangspunt van dit hoofdstuk is dat u al heeft vastgesteld dat u het betreffende datalek moet melden aan de Autoriteit Persoonsgegevens op grond van de meldplicht uit de Wbp. Mocht u dat nog niet hebben vastgesteld, doorloop dan eerst de stappen uit hoofdstuk 4.

Als u het datalek niet meldt aan de betrokkene kan de Autoriteit Persoonsgegevens, indien deze van oordeel is dat de inbreuk waarschijnlijk ongunstige gevolgen zal hebben voor de persoonlijke levenssfeer van de betrokkene, van u verlangen dat u alsnog een kennisgeving doet aan de betrokkenen (artikel 34a, zevende lid, Wbp). Dit staat gelijk aan een bindende aanwijzing.[30] Bij het niet nakomen van een bindende aanwijzing kan de Autoriteit Persoonsgegevens een bestuurlijke boete

[30] Kamerstukken I 2014/15, 33 662, nr. C, blz. 23.

opleggen van ten hoogste het bedrag van de geldboete van de zesde categorie van artikel 23, vierde lid, van het Wetboek van Strafrecht (artikel 66, vijfde lid, Wbp).

### *7.1. Ben ik een financiële onderneming zoals bedoeld in de Wet op het financieel toezicht?*

Voor financiële ondernemingen zoals bedoeld in de Wet op het financieel toezicht (Wft) geldt een uitzondering op de meldplicht voor datalekken aan de betrokkene (artikel 34a, lid 10, Wbp). Als u de betrokkenen informeert, dan doet u dat op grond van uw zorgplicht als financiële onderneming.

### *7.2. Biedt de cryptografie die ik heb toegepast voldoende bescherming om de melding aan de betrokkene achterwege te kunnen laten?*

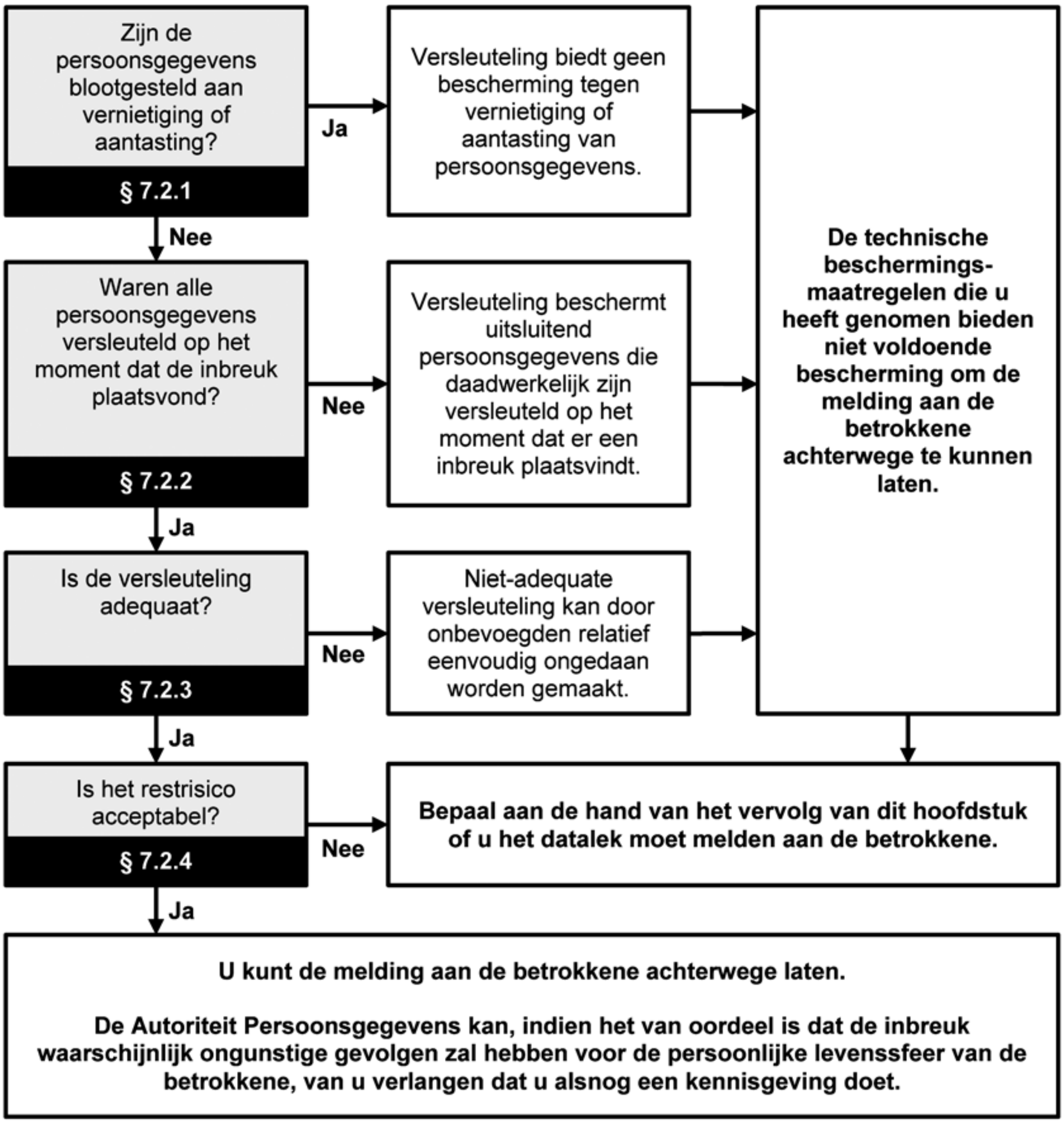
Indien u passende technische beschermingsmaatregelen heeft genomen waardoor de persoonsgegevens die het betreft onbegrijpelijk of ontoegankelijk zijn voor eenieder die geen recht heeft op kennisname van de gegevens, dan kunt u de melding aan de betrokkene achterwege laten (artikel 34a, zesde lid, Wbp).

Uit de wetsgeschiedenis komt de toepassing van cryptografie naar voren als het voornaamste voorbeeld van een technische beschermingsmaatregel zoals bedoeld in het zesde lid van artikel 34a Wbp. Ook artikel 4 van de Europese verordening 611/2013, waarin voor de telecomsector een soortgelijke uitzondering op de meldplicht datalekken aan de betrokkene is opgenomen, gaat uit van de toepassing van cryptografie als technische beschermingsmaatregel. Deze paragraaf gaat in op het gebruik van cryptografie als technische beschermingsmaatregel om persoonsgegevens onbegrijpelijk of ontoegankelijk te maken voor onbevoegden. Andere technische beschermingsmaatregelen worden behandeld in het vervolg van dit hoofdstuk.

Deze paragraaf gaat in op twee cryptografische bewerkingen: encryptie (versleuteling) en hashing (het omzetten van gegevens in een unieke code). Kenmerkend voor encryptie is dat deze bewerking omkeerbaar is: door gebruik van de juiste sleutel kan de oorspronkelijke informatie worden verkregen (decryptie). Encryptie wordt onder meer gebruikt om gegevens te beveiligen die zijn opgeslagen op draagbare apparatuur en op verwijderbare media zoals USB-sticks. Hashing is een bewerking die van informatie, ongeacht de lengte, een unieke hashcode maakt die altijd even lang is (de lengte is afhankelijk van de gebruikte hashingmethode). Hashing wordt onder meer gebruikt bij de opslag en verwerking van wachtwoorden: op het moment dat de gebruiker een (nieuw) wachtwoord kiest, wordt de bijbehorende hashcode opgeslagen. Wanneer de gebruiker vervolgens inlogt, wordt de hashcode van het ingevoerde wachtwoord vergeleken met de opgeslagen hashcode en krijgt de gebruiker toegang tot het informatiesysteem als de codes overeenkomen.

Als door de cryptografische bewerkingen die u heeft toegepast de gelekte persoonsgegevens onbegrijpelijk of ontoegankelijk zijn voor onbevoegden, dan kunt u de melding aan de betrokkene achterwege laten. Dit is een strenge norm, die u van geval tot geval toe moet passen op basis van de actuele stand van de techniek. Als u twijfelt over de adequaatheid van de technische beschermingsmaatregelen die u heeft getroffen, dan moet u het datalek melden aan de betrokkene. Doel van de rest van deze paragraaf is om u bij deze afweging te ondersteunen.[31]

[31] Kamerstukken II 2014/15, 33 662, nr. 11, blz. 9-10.




Iedere vraag uit het bovenstaande schema correspondeert met een van de onderstaande paragrafen.

### *7.2.1. Zijn de persoonsgegevens blootgesteld aan vernietiging of aantasting?*

Persoonsgegevens die adequaat zijn versleuteld kunnen bij een datalek nog steeds worden vernietigd, en ook aantasting of onbevoegde wijziging is nog steeds mogelijk (bijvoorbeeld door zogenoemde 'cryptoware', die de reeds versleutelde gegevens nogmaals versleutelt met een sleutel die de verantwoordelijke uitsluitend tegen betaling in zijn bezit kan krijgen.)

Een datalek waarbij adequaat versleutelde persoonsgegevens niet alleen zijn blootgesteld aan onbevoegde kennisname, maar ook aan verlies of aan andere vormen van onrechtmatige verwerking, kan ongunstige gevolgen hebben voor de persoonlijke levenssfeer van de betrokkene en moet daarom mogelijk aan hem of haar worden gemeld.

**Voorbeeld technische beschermingsmaatregelen bij verlies van persoonsgegevens**[32]
De versleutelde laptop van een financieel adviseur is gestolen uit de kofferbak van zijn auto. Op de laptop staan de financiële dossiers – met daarin onder meer details over hypotheken, salarissen en aanvragen van leningen – van 1000 betrokkenen.
Door de diefstal zijn deze gegevens blootgesteld aan onbevoegde kennisname. De financieel adviseur komt tot de conclusie dat alle gegevens op de harde schijf adequaat versleuteld zijn, en dat het

[32] Bron: Artikel 29-Werkgroep, Advies 03/2014 over kennisgeving bij inbreuken in verband met persoonsgegevens, goedgekeurd op 25 maart 2014, Casus 5.

restrisico acceptabel is. In principe zou hij de melding aan de betrokkene dus achterwege kunnen laten.
Echter: de financieel adviseur beschikt niet over een back-up (reserve-kopie) van de persoonsgegevens op de harde schijf. Dat betekent dat er in dit geval niet alleen sprake is van blootstelling aan onbevoegde kennisname, maar ook van het verlies van de getroffen persoonsgegevens.
Aangezien de financieel adviseur de gegevens niet meer heeft, zal hij ze opnieuw bij de betrokkenen op moeten vragen. De vertraging die hierdoor ontstaat kan ertoe leiden dat deadlines voor de indiening van documenten of aanvragen niet worden gehaald, wat voor de betrokkenen uiteindelijk kan leiden tot boetes, derving van inkomsten of verwachte winst, beëindiging van koopovereenkomsten of andere ingrijpende gevolgen.
In dit geval ligt het, ondanks de genomen technische beschermingsmaatregelen, voor de hand om het datalek te melden aan de betrokkenen. De melding omvat in ieder geval het verzoek om de gegevens opnieuw aan de financieel adviseur te verstrekken en een uitleg van de potentiële consequenties en negatieve gevolgen van de inbreuk.

### *7.2.2. Waren de persoonsgegevens versleuteld op het moment dat de inbreuk plaatsvond?*

Versleuteling beschermt uitsluitend persoonsgegevens die daadwerkelijk versleuteld zijn op het moment dat er een inbreuk plaatsvindt. Een datalek waarbij (ook) niet versleutelde persoonsgegevens zijn gelekt, kan ongunstige gevolgen hebben voor de persoonlijke levenssfeer van de betrokkene en moet daarom mogelijk aan hem of haar worden gemeld.

Voorbeeld persoonsgegevens die niet waren versleuteld op het moment dat de inbreuk plaatsvond
Op de harde schijf van een laptop staat een bestand met persoonsgegevens. Het bestand zelf is niet versleuteld. De laptop wordt automatisch vergrendeld als deze enige tijd niet wordt gebruikt, en bij de automatische vergrendeling wordt de inhoud van de harde schijf versleuteld. De laptop is in handen gekomen van een aanvaller die met technische middelen gebruik van het toetsenbord simuleert, en daardoor voorkomt dat de automatische vergrendeling in werking treedt en de gegevens op de harde schijf worden versleuteld.

**Voorbeeld waarin niet alle getroffen persoonsgegevens waren versleuteld, en de resterende persoonsgegevens niet waren versleuteld op het moment van de inbreuk**[33]
Een werknemer geeft aan een derde de gebruikersnaam en het wachtwoord dat toegang geeft tot alle klantgegevens van alle klanten van het bedrijf waar hij werkt. Het gaat onder meer om namen, adressen, e-mailadressen, telefoonnummers, toegangs- en andere identificatiegegevens (gebruikersnamen, gehashte wachtwoorden en klantnummers) en versleutelde betaalgegevens (waaronder rekeningnummers en creditcardgegevens). Om twee redenen moet de verantwoordelijke dit datalek melden aan de betrokkene:
- slechts een deel van de persoonsgegevens is versleuteld (de wachtwoorden en de betaalgegevens);
- de betaalgegevens zijn weliswaar versleuteld opgeslagen, maar als de derde met de verstrekte gegevens inlogt krijgt hij via de gebruikersinterface toegang tot de onversleutelde gegevens.

### *7.2.3. Is de versleuteling adequaat?*

Het is in eerste instantie aan u om te beoordelen of de versleuteling sterk genoeg is, en op de juiste wijze wordt uitgevoerd.[34]

Zowel encryptie als hashing zijn in principe te 'kraken', wat inhoudt dat onbevoegden toegang kunnen krijgen tot de oorspronkelijke gegevens. Kraken wordt tegengegaan door het gebruik van (combinaties van) moderne cryptografische technieken en door toepassing van zogenoemde salts (extra informatie die bij hashing wordt toegevoegd aan het oorspronkelijke gegeven om het kraken van de hashcode te bemoeilijken). Dit terrein ontwikkelt zich voortdurend en het is zeer goed mogelijk dat een cryptografische bewerking die in de huidige situatie veilig genoeg is dat over enige tijd niet meer is. Bij gebruik van cryptografische bewerkingen beoordeelt u daarom periodiek of deze nog steeds voldoende bescherming bieden.

De Europese verordening 611/2013 geeft een nadere invulling aan adequate versleuteling. Volgens deze verordening mag u gegevens als onbegrijpelijk beschouwen als ze:
- op veilige wijze zijn versleuteld met een standaardalgoritme, de sleutel voor decryptie door geen enkele inbreuk gevaar heeft gelopen en de sleutel voor decryptie zodanig werd gegenereerd dat

33 Bron: Artikel 29-Werkgroep, Advies 03/2014 over kennisgeving bij inbreuken in verband met persoonsgegevens, goedgekeurd op 25 maart 2014, Casus 3.
34 Kamerstukken II 2013/14, 33 662, nr. 6, blz. 31–32.

personen zonder geautoriseerde toegang de sleutel met de beschikbare technologische middelen niet kunnen vinden; of
- zijn vervangen door een met een cryptografisch versleutelde hashfunctie berekende hashwaarde, de sleutel die hiervoor werd gebruikt door geen enkele inbreuk gevaar heeft gelopen en deze voor datahashing gebruikte sleutel zodanig is gegenereerd dat personen zonder geautoriseerde toegang de sleutel niet kunnen vinden met de beschikbare technologische middelen.[35]

Aandachtspunten bij de beoordeling zijn:
- Het algoritme zelf, of de wijze waarop u dit toepast, kunnen kwetsbaarheden vertonen waardoor de encryptie of de hashing niet de bescherming biedt die u daarvan verwacht.
- Encryptie is omkeerbaar. Een onbevoegde die over de juiste sleutel beschikt, of deze zonder al te veel moeite kan vinden, kan de gelekte gegevens ontsleutelen.
- Hashing is herhaalbaar. Als er bij hashing geen salt is toegepast, of als een onbevoegde over de gebruikte salt beschikt of deze zonder al te veel moeite kan vinden, kan hij de gebruikte hashing-methode toepassen op een lijst met veelgebruikte waarden en daardoor bijvoorbeeld gestolen wachtwoorden achterhalen.

Algemene informatie over algoritmen en toepassingen daarvan vindt u onder meer in de publicaties van het European Union Agency for Network and Information Security (ENISA) en het Nationaal Cyber Security Centrum (NCSC). Bij het opstellen van deze beleidsregels was de meest recente publicatie van ENISA op dit gebied het 'Algoritms, key sizes and parameters report – 2014' dat werd gepubliceerd in november 2014.[36]

Behalve het gebruikte algoritme zelf, is voor adequate versleuteling ook van belang dat u dit op de juiste wijze toepast. Een beoordeling door een deskundige kan hier uitsluitsel over bieden. Bij voorkeur vindt deze beoordeling plaats voordat er een datalek heeft plaatsgevonden zodat u, op het moment dat zich een datalek voordoet, gemakkelijk kunt bepalen of de encryptie of de hashing die u heeft toegepast voldoende bescherming biedt.

Als laatste is van belang dat de gebruikte sleutel c.q. salt niet is gelekt. Dit zult u van geval tot geval vast moeten stellen.

### *7.2.4. Is het restrisico acceptabel?*

Door de beantwoording van de voorgaande vragen heeft u, als het goed is, een beeld gekregen van de mate waarin de technische beschermingsmaatregelen die u heeft genomen de gelekte persoonsgegevens beschermen tegen onbevoegde kennisname. Per concreet geval zult u moeten beoordelen of de geboden bescherming voldoende is om de kennisgeving aan de betrokkene achterwege te kunnen laten.

Behalve met wat hierboven is aangegeven, moet u ook meewegen welke gevolgen het voor de persoonlijke levenssfeer van de betrokkene kan hebben als een aanvaller er nu of in de toekomst alsnog in slaagt om kennis te nemen van de getroffen persoonsgegevens.

**Voorbeeld achterwege laten melding betrokkene bij encryptie**
Een laptop, met op de harde schijf een bestand met persoonsgegevens, is gestolen. De verantwoordelijke onderzoekt het incident, en komt tot de conclusie dat hij op grond van het zesde lid van artikel 34a Wbp af mag zien van de melding aan de betrokkene. Zijn overwegingen daarbij zijn:
- bij de versleuteling van het bestand is gebruik gemaakt van combinatie van algoritme en sleutellengte die door het ENISA in een actuele (niet door een recentere publicatie achterhaalde) handreiking wordt beoordeeld als 'toekomst-vast voor de komende 10 tot 50 jaar;
- met betrekking tot het gebruikte algoritme en de implementatie daarvan zijn geen kwetsbaarheden bekend;
- de implementatie is met goed gevolg beoordeeld door een deskundige;
- het bestand zelf was versleuteld, dus de versleuteling was niet afhankelijk van automatische vergrendeling die in het specifieke geval mogelijk niet heeft gewerkt;
- de sleutel is niet gelekt;
- gezien de aard van het datalek, de verwerking en de gelekte gegevens is het restrisico acceptabel.

[35] Artikel 4 Verordening 611/2013.
[36] http://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/algorithms-key-size-and-parameters-report-2014.

### *7.3 Bieden de andere technische beschermingsmaatregelen die ik heb toegepast voldoende bescherming om de melding aan de betrokkene achterwege te kunnen laten?*

Naast encryptie vermeldt de Nederlandse wetsgeschiedenis nog een andere technische beschermingsmaatregel waarmee persoonsgegevens kunnen worden beschermd tegen onbevoegde kennisname: het op afstand wissen van de gegevens die op een apparaat staan (*remote wiping*). Door de gegevens te wissen worden deze ontoegankelijk voor onbevoegden, aangezien na een geslaagde *remote wipe* een eventuele aanvaller nog wel de beschikking heeft over het apparaat waarop de gegevens stonden, maar niet meer over de gegevens zelf. Een *remote wipe* heeft echter uitsluitend kans van slagen als er aan een aantal randvoorwaarden wordt voldaan. De eerste randvoorwaarde is dat de *remote wipe* tijdig in gang wordt gezet, zodat een eventuele aanvaller nog geen kans heeft gehad om kennis te nemen van de gegevens. Verder moet op dat moment het apparaat waar het om gaat nog intact zijn en werken, zodat het in staat is om de *remote wipe* uit te voeren en de gegevens te wissen. Ook moet de toepassing die voor het wissen van de gegevens wordt gebruikt correct werken, zodat alle gegevens waar het om gaat daadwerkelijk worden verwijderd en er ook geen sporen achterblijven waaruit de oorspronkelijke gegevens kunnen worden gereconstrueerd.

Als u gebruik maakt van *remote wiping*, dan zult u op basis van de specifieke omstandigheden van het geval vast moeten stellen of er wordt voldaan aan de strenge norm uit het zesde lid van artikel 34a Wbp. De voorgaande paragrafen kunt u daarbij gebruiken als leidraad.

Ook als de gelekte gegevens gepseudonimiseerd zijn zult u op basis van de specifieke omstandigheden van het geval vast moeten stellen of er aan de norm uit het zesde lid van artikel 34a Wbp wordt voldaan. Pseudonimisering wil zeggen dat u technische maatregelen heeft genomen om te voorkomen dat de persoonsgegevens worden gekoppeld aan de oorspronkelijke identiteit van de betrokkene. Geslaagde pseudonimisering maakt de persoonsgegevens waarover het gaat tot op zekere hoogte onbegrijpelijk voor onbevoegden en de kans dat een datalek ongunstige gevolgen zal hebben voor de persoonlijke levenssfeer van de betrokkene wordt als gevolg daarvan verlaagd. Onvolkomenheden in de wijze waarop de persoonsgegevens zijn gepseudonimiseerd kunnen er echter toe leiden dat onbevoegden de oorspronkelijke identiteit van de betrokkenen alsnog kunnen achterhalen, eventueel met gebruikmaking van andere gegevens die ze reeds in hun bezit hadden of alsnog in hun bezit krijgen.

Net als bij *remote wiping* zult u dus ook bij blootstelling van gepseudonimiseerde gegevens aan onbevoegde kennisname op basis van de specifieke omstandigheden van het geval moeten vaststellen of er wordt voldaan aan de strenge norm uit het zesde lid van artikel 34a Wbp. De onderstaande paragrafen kunt u daarbij gebruiken als leidraad. Verder is aan te bevelen om bij de beoordeling gebruik te maken van het advies over anonimiseringstechnieken dat de samenwerkende Europese toezichthouders in 2014 hebben uitgebracht.[37]

### *7.4. Zal het datalek waarschijnlijk ongunstige gevolgen hebben voor de persoonlijke levenssfeer van de betrokkene?*

Het datalek moet aan de betrokkene worden gemeld indien de inbreuk waarschijnlijk ongunstige gevolgen zal hebben voor diens persoonlijke levenssfeer (artikel 34a, tweede lid, Wbp).

Betrokkenen kunnen door het verlies, onrechtmatig gebruik of misbruik van persoonsgegevens in hun belangen worden geschaad. De schade kan van materiële of van immateriële aard zijn. Bij dit laatste moet u bijvoorbeeld denken aan onrechtmatige publicatie, aantasting in eer en goede naam, identiteitsfraude of discriminatie.[38] Identiteitsfraude kan overigens niet alleen leiden tot immateriële gevolgen, maar ook tot materiële gevolgen.

Het is aan u om te beoordelen of u een datalek aan de betrokkene moet melden.

Indien er **persoonsgegevens van gevoelige aard** zijn gelekt, dan moet u er van uitgaan dat u het datalek niet alleen moet melden aan de Autoriteit Persoonsgegevens, maar ook aan de betrokkene. Verlies of onrechtmatige verwerking van dergelijke gegevens kunnen onder meer leiden tot stigmatisering of uitsluiting van de betrokkene, tot schade aan de gezondheid, financiële schade of (identiteits-)fraude. Meer informatie treft u aan in paragraaf 4.2.1 van deze beleidsregels.

---

37 Artikel 29-Werkgroep, *Advies 5/2014 over anonimiseringstechnieken*, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_nl.pdf.

38 Kamerstukken II 2013/14, 33 662, nr. 6, blz. 19.

In alle overige gevallen zult u op basis van de omstandigheden van het geval een afweging moeten maken.

Het informeren van de betrokkene over een opgetreden datalek is met name noodzakelijk in situaties waarin er voor hem of haar daadwerkelijk ongunstige gevolgen voor de persoonlijke levenssfeer te duchten zijn. Door de kennisgeving is de betrokkene alert op de mogelijke gevolgen van het datalek en kan hij of zij zich, voor zover dat mogelijk is, daartegen wapenen door bijvoorbeeld extra voorzorgsmaatregelen te treffen (zoals vervanging van een wachtwoord) of door diensten of producten van een andere marktpartij af te nemen.[39]

**Voorbeelden van datalekken die moeten worden gemeld aan de betrokkene**[40]

1. Vier laptops zijn gestolen bij een gezondheidscentrum voor kinderen. De laptops bevatten gevoelige gegevens over gezondheid en welzijn en andere persoonsgegevens van meer dan 2000 kinderen.
   *Gelet op de mogelijke gevolgen van het datalek is kennisgeving aan de betrokkenen geboden. Daarbij is het wel belangrijk om rekening te houden met de leeftijd en de rijpheid van de betrokkenen. Naast de kennisgeving aan het kind zelf, voor zover deze passend is, kan het in dit geval juister zijn om een ouder of voogd, die al actief betrokken is bij de medische verzorging van het kind, op de hoogte te brengen.*
   *Door de kwijtgeraakte gegevens kan de integriteit van de medische dossiers worden aangetast, wat de behandeling van de kinderen kan verstoren. Als de ouders of verzorgers op de hoogte zijn van het datalek dan kunnen ze hier alert op zijn, en kunnen ze bij eventuele afwijkingen in de medische zorg voor hun kinderen contact opnemen met de betreffende zorgverlener.*
2. Bij een levensverzekeraar waren persoonsgegevens ongeoorloofd ingezien als gevolg van een kwetsbaarheid in een webapplicatie. Van 700 personen konden naam, adres en formulieren met medische gegevens worden ingezien.
   *Als de aanvaller buitgemaakte gegevens op internet zet kan dat er bijvoorbeeld toe leiden dat betrokkenen moeilijker een baan kunnen vinden, als gevolg van het bekend worden van informatie over gezondheidsproblemen, zwangerschap, etc. Betrokkenen kunnen ook te maken krijgen met phishing of identiteitsfraude. Het datalek heeft waarschijnlijk negatieve gevolgen voor de betrokkenen, die er daarom van in kennis moeten worden gesteld.*
3. Een medewerker van een internetprovider heeft zijn login/wachtwoordgegevens aan een derde partij gegeven die daardoor nagenoeg onbeperkt bij alle klantgegevens (meer dan 100.000) kon komen. Het kan niet redelijkerwijs worden uitgesloten dat er daadwerkelijk persoonsgegevens verloren zijn gegaan of onrechtmatig zijn verwerkt.
   *De derde partij had onder meer toegang tot betaalgegevens (waaronder creditcardinformatie) en hashwaarden van wachtwoorden van klanten. Misbruik van de betaalgegevens kan financiële gevolgen hebben voor de klanten. Ook is het mogelijk dat de onbevoegde derde op basis van de buitgemaakte hashwaarden de oorspronkelijke wachtwoorden van de klanten kan achterhalen. Het datalek heeft waarschijnlijk negatieve gevolgen voor de betrokkenen, die er daarom van in kennis moeten worden gesteld. Als de wachtwoorden niet meer veilig zijn, dan moet de verantwoordelijke de klanten op een veilige manier verplichten om een nieuw wachtwoord aan te maken. Hij moet daarbij zorgen dat de nieuwe wachtwoorden worden aangemaakt door legitieme gebruikers, en niet door derden die de inloggegevens hebben bemachtigd. Hij moet daarbij ook aangeven wat de reden is voor de vervanging van het wachtwoord.*
4. Een envelop met creditcardbetalingsgegevens van 800 personen was per ongeluk niet versnipperd, maar in een vuilnisbak gegooid. Een derde persoon haalde de gegevens uit de vuilniscontainer op straat en verstrekte ze aan andere personen.
   *Het datalek kan financiële consequenties hebben voor de betrokkenen, als hun kaartgegevens nog geldig zijn en worden misbruikt. De betrokkenen moeten daarom van het datalek in kennis worden gesteld.*
5. De versleutelde laptop van een financieel adviseur is uit de auto gestolen. Financiële gegevens (hypotheken, salarissen, leningen) van 1000 personen waren betrokken. Hoewel het wachtwoord van de laptop niet gecompromitteerd is, was er geen back-up voorhanden.
   *Aangezien de verantwoordelijke niet meer beschikt over de persoonsgegevens die op de laptop stonden, zullen deze opnieuw door de betrokkenen moeten worden verstrekt. Op zich heeft dit slechts beperkte negatieve gevolgen voor de betrokkenen: er is hooguit sprake van frustratie en tijdverspilling omdat ze alle informatie nogmaals moeten verzamelen. In sommige gevallen kunnen ook deadlines voor de indiening van documenten of aanvragen worden overschreden, wat*

[39] Kamerstukken II 2014/15, 33 662, nr. 11, blz. 6.
[40] Volledigheidshalve zijn hier ook de voorbeelden opgenomen die betrekking hebben op de telecomsector. De voorbeelden zijn ontleend aan Advies 03/2014 over kennisgeving bij inbreuken in verband met persoonsgegevens, goedgekeurd op 25 maart 2014, van de Artikel 29-Werkgroep. In dit advies is per voorbeeld een meer uitgebreide uitwerking opgenomen, met daarbij ook maatregelen waarmee het datalek had kunnen worden voorkomen of de negatieve gevolgen hadden kunnen worden beperkt.

*kan leiden tot financiële schade voor de betrokkenen. De betrokkenen moeten van het datalek in kennis worden gesteld. In de kennisgeving moet worden aangegeven dat de gegevens opnieuw aan de financieel adviseur moeten worden verstrekt, en moet uitleg worden gegeven over de potentiële consequenties en mogelijke negatieve gevolgen van het datalek.*

6. Op de website van een telefoonbedrijf kunnen klanten inloggen en hun financiële gegevens en belgegevens inzien. Een derde partij heeft toegang gekregen tot de database met inlognamen en bijbehorende hashwaarden van wachtwoorden. Bij het hashen van de wachtwoorden is gebruik gemaakt van een verouderd algoritme dat onvoldoende bescherming biedt tegen kennisname door onbevoegden. Gevolg is dat een derde partij de oorspronkelijke wachtwoorden zonder al te veel moeite zal kunnen achterhalen.
   *[Dit voorbeeld heeft betrekking op de telecomsector, en valt dus niet onder de meldplicht datalekken uit de Wbp. De overwegingen bij het informeren van de betrokkenen kunnen echter ook buiten de telecomsector worden toegepast.] De derde partij kan de wachtwoorden van alle abonnees achterhalen. Hij beschikt ook over de inlognamen, en kan zich daardoor toegang verschaffen tot alle accounts. Veel mensen gebruiken voor het inloggen op meerdere websites dezelfde combinatie van inlognaam en wachtwoord. Dit betekent dat de derde zich met de buitgemaakte gegevens mogelijk ook toegang kan verschaffen tot andere accounts van sommige betrokkenen, waaronder mogelijk ook e-mailaccounts. Dit datalek heeft waarschijnlijk negatieve gevolgen voor de betrokkenen, en kennisgeving is vereist. De klanten moeten op de hoogte worden gesteld van het datalek, met daarbij het dringende advies om voor alle accounts waar ze hetzelfde wachtwoord gebruiken, dit wachtwoord aan te passen. Ze moeten bij het inloggen op de website in kwestie ook worden gedwongen om hun wachtwoord voor de kwestie aan te passen. Daarbij moet worden gezorgd dat de nieuwe wachtwoorden worden aangemaakt door legitieme gebruikers, en niet door derden die de inloggegevens hebben bemachtigd.*
7. Een internetprovider biedt de gebruikers de mogelijkheid om details van hun account te zien, zoals onder andere historische zoekgegevens en vaak bezochte websites. Door een fout in de website had eenieder via een simpele truc de mogelijkheid om de accounts van andere gebruikers vrijelijk in te zien. Zonder een sluitende logging is hier niet vast te stellen of dat daadwerkelijk is gebeurd en welke gegevens dan zijn geraadpleegd.
   *[Dit voorbeeld heeft betrekking op de telecomsector, en valt dus niet onder de meldplicht datalekken uit de Wbp. De overwegingen bij het informeren van de betrokkenen kunnen echter ook buiten de telecomsector worden toegepast.] De gegevens kunnen worden gebruikt voor het versturen van spam aan de betrokkenen of voor telefonische verkoop of phishing. De buitgemaakte gegevens kunnen mogelijk ook worden gebruikt om profielen van de klanten op te stellen of hun gedragingen in kaart te brengen, wat gevoelige informatie aan het licht zou kunnen brengen. Dit datalek heeft waarschijnlijk negatieve gevolgen voor de betrokkenen, en moet daarom aan hen worden gemeld.*

### *7.5. Zijn er zwaarwegende redenen om de melding aan de betrokkene achterwege te laten?*

U mag de melding aan de betrokkene achterwege laten, als daarvoor zwaarwegende redenen aanwezig zijn (artikel 43 Wbp). Daarbij geldt wel dat de melding aan de betrokkene alleen achterwege mag blijven als dit *noodzakelijk* is met het oog op de belangen die worden genoemd in dit artikel.

Op grond van artikel 43, onder e, Wbp mag van de melding aan de betrokkene worden afgezien voor zover dit noodzakelijk is in het belang van de bescherming van de betrokkene.

**Voorbeeld achterwege laten melding i.v.m. bescherming betrokkene**
Er zijn gegevens gelekt over medische en psychosociale hulpvragen die kinderen buiten medeweten van hun ouders hebben gedaan. De verantwoordelijke meldt het datalek aan de Autoriteit Persoonsgegevens, en beroept zich op artikel 43, onder e, Wbp om de melding aan de betrokkenen achterwege te kunnen laten. Reden is dat de ouders door de melding op de hoogte zouden kunnen raken van de hulpvraag.

Het melden van datalekken aan de betrokkenen brengt administratieve lasten met zich mee, maar op zichzelf is dat geen reden om de melding achterwege te laten. Alleen als u aannemelijk kunt maken dat de administratieve lasten die zijn gemoeid met het melden van het datalek aan de betrokkene zodanig disproportioneel zijn dat u in een van uw rechten en vrijheden wordt aangetast of dreigt te worden aangetast, dan kunt u een beroep doen op artikel 43, onder e, Wbp om melding aan de betrokkene achterwege te laten.

**Voorbeeld achterwege laten melding i.v.m. rechten en vrijheden verantwoordelijke**[41]
Een beursgenoteerde onderneming is verwikkeld in een overname op het moment dat zich een groot

[41] Kamerstukken II, 2013/14, 33 662, blz. 8.

datalek voordoet. De onderneming meldt het datalek aan de Autoriteit Persoonsgegevens, en beroept zich op artikel 43, onder e, Wbp om de melding aan de betrokkene (voorlopig) achterwege te kunnen laten.

## 8. Hoe moet ik het datalek melden aan de betrokkene?

In de kennisgeving aan de betrokkene vermeldt u in ieder geval: de aard van de inbreuk, de instanties waar de betrokkene meer informatie over de inbreuk kan krijgen, en de maatregelen die u de betrokkene aanbeveelt om te nemen om de negatieve gevolgen van de inbreuk te beperken (artikel 34a, derde lid, Wbp).

Bij het beschrijven van de aard van de inbreuk kunt u doorgaans met een algemene omschrijving volstaan. U neemt uw contactgegevens op zodat de betrokkene u kan bereiken als hij of zij vragen heeft over het datalek. Verder geeft u aan wat de betrokkene zelf kan doen om de negatieve gevolgen van het datalek te beperken. U moet daarbij denken aan het veranderen van gebruikersnamen en wachtwoorden wanneer deze door de inbreuk mogelijk gecompromitteerd zijn. Het staat u vrij om meer informatie toe te voegen aan de kennisgeving, maar dit is niet verplicht.[42]

**Voorbeeld melding aan de betrokkene en vervolgacties**[43]
Een energieleverancier biedt zijn klanten een online account aan waarop ze kunnen inloggen om recente facturen en verbruiksinformatie te raadplegen. Het bedrijf ontdekt dat een derde zich illegaal toegang heeft verschaft tot de database met gebruikersnamen en wachtwoorden van de website. De wachtwoorden zijn niet adequaat versleuteld.

De energieleverancier onderneemt de volgende acties:
- hij informeert zijn klanten over het datalek. Hij beveelt daarbij aan om, voor alle accounts waar de klant hetzelfde wachtwoord gebruikt, dit wachtwoord te wijzigen;
- hij reset alle wachtwoorden en dwingt alle gebruikers om een nieuw wachtwoord op te geven. Hij doet dit op een veilige manier zodat hij zeker weet dat het zijn klanten zijn die een nieuw wachtwoord aanmaken, en niet een onbevoegde derde, en hij geeft hierbij ook aan waarom de klant een nieuw wachtwoord aan moet maken;
- hij past zijn systemen aan, zodat alle gebruikte wachtwoorden op een adequate manier worden versleuteld.

U doet de kennisgeving aan de betrokkene op zo'n manier dat, rekening houdend met de aard van de inbreuk, de geconstateerde en de feitelijke gevolgen daarvan voor de verwerking van persoonsgegevens, de kring van betrokkenen en de kosten van tenuitvoerlegging, een behoorlijke en zorgvuldige informatievoorziening is gewaarborgd (artikel 34a, lid 5 Wbp).

In veruit de meeste gevallen zult u als verantwoordelijke beschikken over de contactgegevens van de betrokkenen, en zult u in staat zijn om de betrokkenen individueel te informeren.

Bij meer omvangrijke incidenten kunt u kiezen voor een combinatie van algemene voorlichting en het op individuele basis informeren van betrokkenen. Bijvoorbeeld:
- U stuurt een e-mail naar de betrokkenen waarin u kort aangeeft wat er is gebeurd en wat de betrokkene zelf kan doen om de negatieve gevolgen tegen te gaan.
- In de e-mail aan de betrokkenen verwijst u naar meer uitgebreide informatie op uw website. Daar licht u de aard van de inbreuk en de maatregelen die de betrokkene zelf kan treffen waar nodig nader toe.
- Verder verwijst u in de e-mail naar een centraal informatiepunt (e-mail, telefoonnummer) waar de betrokkene nadere informatie kan verkrijgen.

Het belangrijkste is, dat u zo veel mogelijk betrokkenen bereikt met informatie die hen helpt om de gevolgen van het datalek voor hun persoonlijke levenssfeer zo veel mogelijk te beperken. Met enkel een bericht in de media wordt dat doel normaal gesproken niet bereikt.[44]

## 9. Wanneer moet ik het datalek melden aan de betrokkene?

U moet het datalek onverwijld melden aan de betrokkene (artikel 34a, tweede lid, Wbp).

---

[42] Kamerstukken II, 2012/13, 33 662, nr. 3, blz. 21-22.
[43] Bron: Artikel 29-Werkgroep, Advies 03/2014 over kennisgeving bij inbreuken in verband met persoonsgegevens, goedgekeurd op 25 maart 2014, Casus 6.
[44] Kamerstukken I, 2014/15, 33 662, nr. C, blz. 15.

Het onverwijld melden houdt in dat u, na het ontdekken van het datalek, enige tijd mag nemen voor nader onderzoek zodat u de betrokkene op een behoorlijke en zorgvuldige manier kunt informeren. Wel moet u er rekening mee houden dat de betrokkene naar aanleiding van uw melding mogelijk maatregelen moet nemen om zich te beschermen tegen de gevolgen van het datalek. Hoe eerder u de betrokkene daarover informeert, hoe eerder deze in actie kan komen.

Net als bij de melding aan de Autoriteit Persoonsgegevens kunt u er eventueel voor kiezen om de betrokkene in eerste instantie te informeren op basis van de informatie waarover u op dat moment beschikt, zodat deze alvast maatregelen kan gaan treffen om zich te beschermen tegen de gevolgen van het datalek, en om deze informatie in tweede instantie op basis van nader onderzoek aan te vullen. Een voorbeeld van een dergelijke situatie is dat u weet dat onbevoegden toegang hebben gehad tot een database met inloggegevens, maar dat u nog aan het onderzoeken bent of de onbevoegden ook andere persoonsgegevens hebben ingezien. U kunt in een dergelijk geval meteen al beginnen met het resetten van de getroffen wachtwoorden en met het informeren van de betrokkenen, waarbij u aangeeft dat betrokkenen, als zij elders dezelfde inloggegevens gebruiken, deze moeten wijzigen.

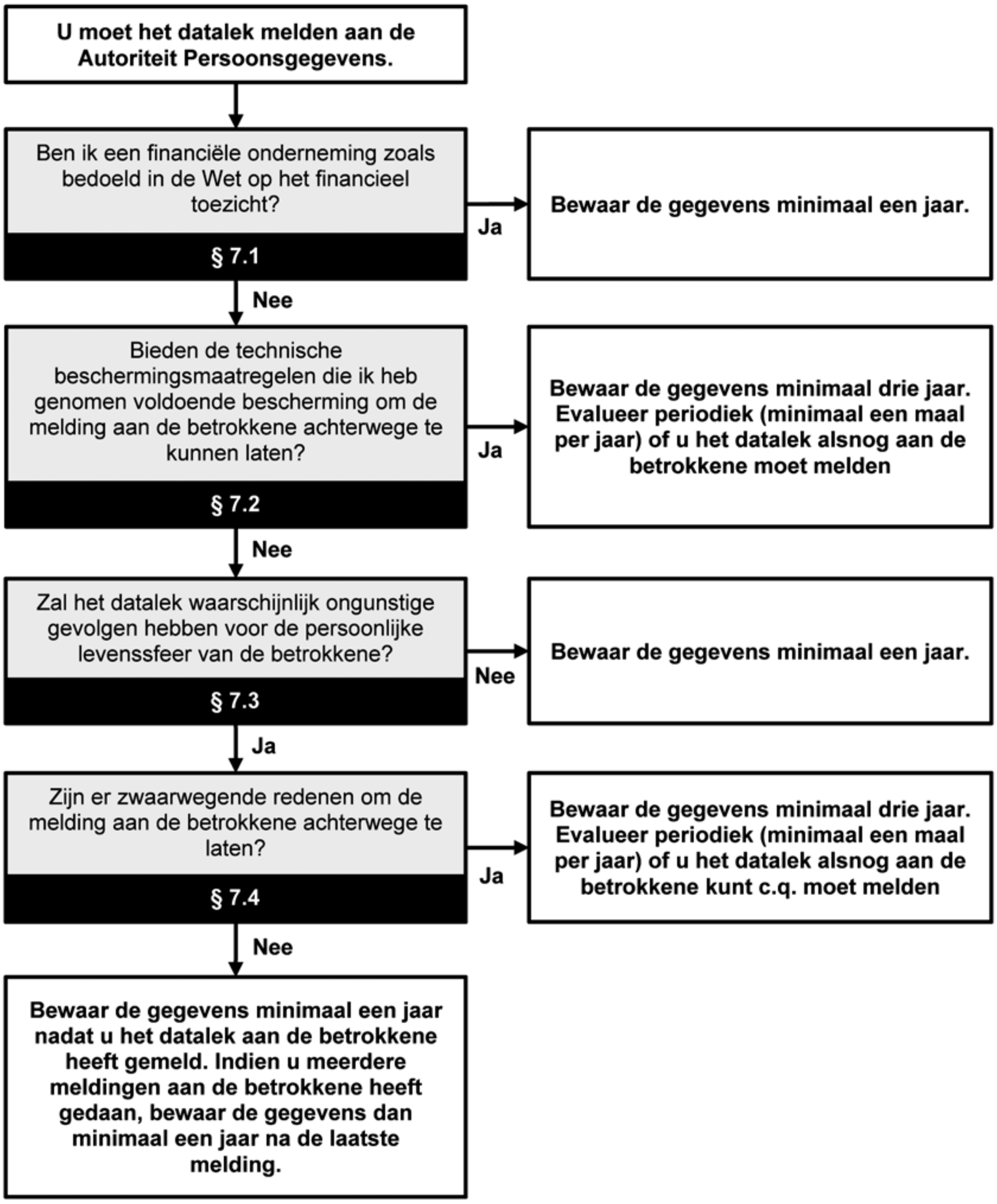
In de melding aan de Autoriteit Persoonsgegevens moet u aangeven of u het datalek al aan de betrokkenen heeft gemeld en, zo niet, wanneer u dat gaat doen. De termijn die u in de melding aan de Autoriteit Persoonsgegevens aangeeft, moet u ook nakomen. Mocht deze termijn bij nader inzien niet haalbaar blijken te zijn, dan laat u dit aan de Autoriteit Persoonsgegevens weten door middel van een aanpassing van de melding.

### 10. Welke gegevens moet ik vastleggen over dit datalek?

U moet een overzicht bijhouden van alle datalekken die onder de meldplicht vallen. Per datalek bevat het overzicht in ieder geval feiten en gegevens omtrent de aard van de inbreuk. Als het datalek is gemeld aan de betrokkene, dan neemt u ook de tekst van de kennisgeving aan de betrokkene in het overzicht op (artikel 34a lid 8 Wbp).

De wet schrijft niet voor hoe lang u het overzicht moet bewaren. Ga uit van een bewaartermijn van **minimaal een jaar**. In bepaalde gevallen kan het nodig zijn om een langere bewaartermijn te hanteren.[45] Het onderstaande schema biedt u hiervoor een beslismodel.

[45] Handelingen I 2014/15, nr. 12, blz. 5.




U hoeft uitsluitend gegevens vast te leggen over datalekken die onder de meldplicht vallen. Mocht u nog niet hebben vastgesteld of het betreffende datalek onder de meldplicht valt, doorloop dan eerst de stappen uit hoofdstuk 3 van deze beleidsregels.

De vragen uit het bovenstaande schema worden nader toegelicht in hoofdstuk 7 van deze beleidsregels.

Het bovenstaande schema gaat ervan uit dat u de gegevens voor de volgende doeleinden bewaart:
- lering trekken uit het datalek en uit de wijze waarop u dit heeft afgehandeld;
- antwoord kunnen geven op vragen van betrokkenen en anderen;
- alsnog melden van het datalek aan de betrokkenen, indien u dit in eerste instantie achterwege hebt gelaten en de omstandigheden vereisen dat u dit alsnog doet.

Dit laatste kan zich bijvoorbeeld voordoen als u bij diefstal van een versleutelde dataset op grond van het zesde lid van artikel 34a Wbp besluit om de kennisgeving aan de betrokkene achterwege te laten. U moet zich er in een dergelijke situatie van bewust zijn dat de komst van nieuwe technieken nieuwe risico's kan inhouden, en dat er met grote regelmaat nieuwe kwetsbaarheden in breed gebruikte versleutelingsalgoritmen worden ontdekt. Dit houdt in dat u, met de diefstal van de versleutelde

dataset in het achterhoofd, over een langere periode alert moet zijn op deze risico's. Bij signalen van mogelijke ontsleuteling zult u alsnog de afweging moeten maken of u de betrokken personen moet informeren.[46]

Houdt u er verder rekening mee dat een vervolgprocedure na een datalek juridische maatregelen kan omvatten (civiel- of strafrechtelijk), en dat u waar dat aan de orde is het bewijsmateriaal moet verzamelen, bewaren en presenteren overeenkomstig de voorschriften voor bewijs die voor het relevante rechtsgebied zijn vastgelegd.

U hoeft het overzicht niet openbaar te maken.

## 11. Wat doet de Autoriteit Persoonsgegevens met mijn melding?

Dit hoofdstuk geeft antwoord op de vraag wat de Autoriteit Persoonsgegevens doet met uw datalek-melding. Ook gaat dit hoofdstuk in op de handhaving bij overtreding van de meldplicht.

### *11.1 Administratieve afhandeling*

Na het melden van een datalek ontvangt u per omgaande een ontvangstbevestiging.

Als de melding de Autoriteit Persoonsgegevens aanleiding geeft tot nadere actie, dan zal de deze daarover contact met u opnemen. In eerste instantie zal het daarbij gaan om verificatie dat de gedane melding daadwerkelijk van u afkomstig is, en om eventuele inhoudelijke vragen over de melding.

### *11.2 Inhoudelijke afhandeling*

Het is uw verantwoordelijkheid om de oorzaak van het datalek op te sporen, en om maatregelen te treffen om herhaling te voorkomen. Het is ook aan u om te bepalen of u de betrokkenen informeert en op welke manier u dit doet. Een van de doelen van deze beleidsregels is om u bij deze afweging te ondersteunen. De Autoriteit Persoonsgegevens biedt, als toezichthouder, geen ondersteuning bij de afhandeling van een concreet datalek.

De ontvangen datalekmeldingen stellen de Autoriteit Persoonsgegevens in staat om erop toe te zien dat betrokkenen adequaat worden geïnformeerd over datalekken die hen persoonlijke raken, of waarvan zij last kunnen ondervinden. Als u het datalek niet heeft gemeld aan de betrokkene kan de Autoriteit Persoonsgegevens, indien deze van oordeel is dat het datalek waarschijnlijk ongunstige gevolgen zal hebben voor de betrokkene, van u verlangen dat u alsnog een kennisgeving doet (artikel 34a, zevende lid, Wbp). Dit staat gelijk aan een bindende aanwijzing, en het niet-nakomen kan worden bestraft met een bestuurlijke boete.[47]

Ook kan de Autoriteit Persoonsgegevens op basis van de ontvangen datalekmeldingen actie onderne-men om de adequate beveiliging van persoonsgegevens meer in de breedte te bevorderen. Als uit de ontvangen datalekmeldingen blijkt dat de beveiliging van persoonsgegevens mogelijk niet op orde is, dan kan dat voor de Autoriteit Persoonsgegevens aanleiding vormen voor nader onderzoek naar de naleving van de beveiligingsverplichtingen uit de Wbp.

### *11.3 Register van ontvangen datalekmeldingen*

De Autoriteit Persoonsgegevens houdt een register bij van de ontvangen datalekmeldingen. Dit register is niet openbaar. Het belang bij het vertrouwelijk blijven van gegevens over de beveiliging van de gegevensverwerking of over gelekte persoonsgegevens staat daaraan in de weg. Wel kan de Autoriteit Persoonsgegevens op basis van de gedane meldingen in jaarverslagen of andere publicaties op geanonimiseerd en geaggregeerd niveau aandacht besteden aan datalekken.[48]

De Autoriteit Persoonsgegevens houdt toezicht op de naleving van de wettelijke regels voor bescher-ming van persoonsgegevens. Onder meer kan de Autoriteit Persoonsgegevens onderzoek doen naar mogelijke overtredingen van de wet (artikel 60 Wbp). Heeft de Autoriteit Persoonsgegevens tijdens het onderzoek overtredingen geconstateerd die voortduren, dan kan deze handhavend optreden (artikel 65 en 66 Wbp). Daarbij kan de Autoriteit Persoonsgegevens gebruik maken van informatie uit ontvangen datalekmeldingen. Op eventuele publicatie van deze informatie zijn de Beleidsregels actieve openbaar-making door de Autoriteit Persoonsgegevens van toepassing.

---

[46] Kamerstukken II, 2014/15, 33 662, nr. 11, blz. 10.
[47] Kamerstukken I 2014/15, 33 662, nr. C, blz. 23.
[48] Kamerstukken II 2013/14, 33 662, nr. 6, blz. 32–33.

De Autoriteit Persoonsgegevens kan samenwerkingsafspraken maken met andere toezichthouders. Deze afspraken worden vastgelegd in een samenwerkingsprotocol, dat wordt gepubliceerd in de Staatscourant (artikel 51a lid 1 Wbp). In het kader van deze afspraken kan de Autoriteit Persoonsgegevens ook informatie uit ontvangen datalekmeldingen doorgeven aan deze toezichthouders (artikel 51a lid 2 Wbp).

### *11.4 Handhaving*

Bij overtreding van datgene dat bij of krachtens artikel 34a Wbp wordt bepaald, kan de Autoriteit Persoonsgegevens een bestuurlijke boete opleggen. Deze bestuurlijke boete bedraagt ten hoogste het bedrag van de zesde categorie van artikel 23, vierde lid, van het Wetboek van Strafrecht (artikel 66, tweede lid, Wbp).

Als sprake is van een overtreding van de Wbp die opzettelijk is gepleegd of het gevolg is van ernstig verwijtbare nalatigheid, kan de toezichthouder direct een bestuurlijke boete opleggen (artikel 66, vierde lid, Wbp). Onder 'ernstig verwijtbare nalatigheid' wordt in de parlementaire geschiedenis verstaan: "[...] grof, aanzienlijk onzorgvuldig, onachtzaam dan wel onoordeelkundig handelen. Indien meerdere malen eenzelfde type overtreding heeft plaatsgevonden, kan sneller worden aangenomen dat sprake is van nalatigheid."[49]

Indien er geen sprake is van een overtreding van de Wbp die opzettelijk is gepleegd of het gevolg is van ernstig verwijtbare nalatigheid, gaat een bindende aanwijzing vooraf aan het opleggen van een bestuurlijke boete. De Autoriteit Persoonsgegevens kan de overtreder een termijn stellen waarbinnen de aanwijzing moet worden opgevolgd (artikel 66, derde lid, Wbp). Bij het niet nakomen van een bindende aanwijzing kan de Autoriteit Persoonsgegevens een bestuurlijke boete opleggen van ten hoogste het bedrag van de geldboete van de zesde categorie van artikel 23, vierde lid, van het Wetboek van Strafrecht (artikel 66, vijfde lid, Wbp).

Bij het opleggen van een bestuurlijke boete houdt de Autoriteit Persoonsgegevens rekening met alle omstandigheden van het geval. Een omstandigheid van het geval kan bestaan uit het feit dat de gegevens waarover het gaat niet door derden zijn ingezien en de privacybelangen van de betrokkenen niet daadwerkelijk zijn geschaad.[50]

---

[49] Kamerstukken II 2013/14, 33 662, nr. 16, blz. 1.
[50] Kamerstukken II 2014/15, 33 662, nr. 24.

## BIJLAGE: GEGEVENS IN DE MELDING

Deze bijlage bevat de gegevens die u op moet geven als u een datalek meldt aan de Autoriteit Persoonsgegevens. Bij het formulier zijn de vragen uit bijlage I bij de Europese Verordening 611/2013 als uitgangspunt gehanteerd. Binnen Europa wordt gestreefd naar harmonisatie van de wijze waarop datalekken in de telecomsector aan de toezichthouder moeten worden gemeld.[51] Op het moment dat dit streven leidt tot concrete resultaten, dan zal de Autoriteit Persoonsgegevens daar uiteraard bij aansluiten.

### Aard van de melding

1) Is dit een vervolg op een eerdere melding? (Kies een van de volgende opties.)
   a) Ja
   b) Nee
2) Wat is het nummer van de oorspronkelijke melding? (Beantwoord deze vraag als u vraag 1 met ja hebt beantwoord.)
3) Wat is de strekking van de vervolgmelding? (Beantwoord deze vraag als u vraag 1 met ja hebt beantwoord, kies een van de volgende opties.)
   a) Toevoegen of wijzigen van informatie betreffende de eerdere melding
   b) Intrekking van de eerdere melding
4) Wat is de reden van intrekking? (Beantwoord deze vraag als u bij vraag 3 gekozen heeft voor optie b.)

### Wettelijk kader voor de melding

5) Op grond van welke wettelijke bepaling doet u deze melding?[52]
   a) artikel 34a, eerste lid, van de Wbp
   b) artikel 11.3a, eerste lid, van de Tw

### Algemene informatie en contactgegevens

6) Over welk bedrijf of welke organisatie gaat het? (Vul de onderstaande gegevens in.)
   a) Naam van het bedrijf of de organisatie
   b) (Bezoek)adres
   c) Postcode
   d) Plaats
   e) KvK-nummer
7) Door wie wordt het datalek gemeld? (Vul de onderstaande gegevens in.)
   a) Naam van de persoon die meldt
   b) Functie van de persoon die meldt
   c) E-mailadres van de persoon die meldt
   d) Telefoonnummer van de persoon die meldt
   e) Alternatief telefoonnummer van de persoon die meldt
8) Met wie kan de Autoriteit Persoonsgegevens contact opnemen voor nadere informatie over de melding? (Vul de onderstaande gegevens in indien dit iemand anders is dan de melder van het datalek.)
   a) Naam contactpersoon
   b) Functie van de contactpersoon
   c) E-mailadres van de contactpersoon
   d) Telefoonnummer van de contactpersoon
   e) Alternatief telefoonnummer van de contactpersoon
9) In welke sector is het bedrijf of de organisatie actief? (Kies een van de onderstaande opties.)
   a) …[53]

### Gegevens over het datalek

10) Geef een samenvatting van het incident waarbij de inbreuk op de beveiliging van persoonsgegevens zich heeft voorgedaan.
11) Van hoeveel personen zijn persoonsgegevens betrokken bij de inbreuk? (Vul de aantallen in.)
   a) Minimaal: (vul aan)

[51] Verordening 611/2013, considerans 11.
[52] Zie paragraaf 4.1 van deze richtsnoeren.
[53] Doel van deze vraag is om mediaberichten en andere signalen over opgetreden datalekken zo goed mogelijk te kunnen matchen met de ontvangen datalekmeldingen.

b) Maximaal: (vul aan)
12) Omschrijf de groep mensen van wie persoonsgegevens zijn betrokken bij de inbreuk.
13) Wanneer vond de inbreuk plaats? (Kies een van de volgende opties en vul waar nodig aan.)
    a) Op (datum)
    b) Tussen (begindatum periode) en (einddatum periode)
    c) Nog niet bekend
14) Wat is de aard van de inbreuk? (U kunt meerdere mogelijkheden aankruisen.)
    a) Lezen (vertrouwelijkheid)
    b) Kopiëren
    c) Veranderen (integriteit)
    d) Verwijderen of vernietigen (beschikbaarheid)
    e) Diefstal
    f) Nog niet bekend
15) Om welk type persoonsgegevens gaat het? (U kunt meerder mogelijkheden aankruisen.)
    a) Naam-, adres- en woonplaatsgegevens
    b) Telefoonnummers
    c) E-mailadressen of andere adressen voor elektronische communicatie
    d) Toegangs- of identificatiegegevens (bijvoorbeeld inlognaam / wachtwoord of klantnummer)
    e) Financiële gegevens (bijvoorbeeld rekeningnummer, creditcardnummer)
    f) Burgerservicenummer (BSN) of sofinummer
    g) Paspoortkopieën of kopieën van andere legitimatiebewijzen
    h) Geslacht, geboortedatum en/of leeftijd
    i) Bijzondere persoonsgegevens (bijvoorbeeld ras, etniciteit, criminele gegevens, politieke overtuiging, vakbondslidmaatschap, religie, seksuele leven, medische gegevens)
    j) Overige gegevens, namelijk (vul aan)
16) Welke gevolgen kan de inbreuk hebben voor de persoonlijke levenssfeer van de betrokkenen? (U kunt meerdere mogelijkheden aankruisen.)
    a) Stigmatisering of uitsluiting
    b) Schade aan de gezondheid
    c) Blootstelling aan (identiteits)fraude
    d) Blootstelling aan spam of phishing
    e) Anders, namelijk (vul aan)

### Vervolgacties naar aanleiding van het datalek

17) Welke technische en organisatorische maatregelen heeft uw organisatie getroffen om de inbreuk aan te pakken en om verdere inbreuken te voorkomen?

### Inlichten van de betrokkenen

18) Heeft u het datalek gemeld aan de betrokkenen of bent u van plan dat te gaan doen? (Kies een van de volgende opties.)
    a) Ja
    b) Nee
    c) Nog niet bekend
19) Wanneer heeft u het datalek gemeld aan de betrokkenen, of wanneer gaat u dit doen? (Beantwoord deze vraag als u vraag 18 met ja hebt beantwoord. Kies een van de volgende opties en vul waar nodig aan.)
    a) Ik heb het datalek aan de betrokkenen gemeld op (datum)
    b) Ik ga het datalek aan de betrokkenen melden op (datum)
    c) Nog niet bekend
20) Wat is de inhoud van de melding aan de betrokkenen? (Letterlijke weergave, beantwoord deze vraag als u vraag 18 met ja hebt beantwoord.)
21) Hoe veel betrokkenen heeft u in kennis gesteld of gaat u in kennis stellen? (Beantwoord deze vraag als u vraag 18 met ja hebt beantwoord.)
22) Welk communicatiemiddel of welke communicatiemiddelen gebruikt u of gaat u gebruiken bij het in kennis stellen van de betrokkenen? (Beantwoord deze vraag als u vraag 18 met ja hebt beantwoord.)
23) Waarom ziet u af van het melden van het datalek aan de betrokkenen? (Beantwoord deze vraag als u vraag 18 met nee hebt beantwoord. Kies een van de onderstaande opties en vul waar nodig aan.)
    a) De technische beschermingsmaatregelen die ik heb getroffen bieden voldoende bescherming om de melding aan de betrokkene achterwege te kunnen laten[54]

[54] Zie paragraaf 7.2 van deze richtsnoeren.

b) Het is onwaarschijnlijk dat het datalek ongunstige gevolgen zal hebben voor de persoonlijke levenssfeer van de betrokkene, want: (vul aan)[55]
c) Ik heb zwaarwegende redenen om de melding aan de betrokkene achterwege te laten, namelijk: (vul aan)[56]
d) Anders, namelijk: (vul aan)

### Technische beschermingsmaatregelen

24) Zijn de persoonsgegevens versleuteld, gehasht of op een andere manier onbegrijpelijk of ontoegankelijk gemaakt voor onbevoegden?[57] (Kies een van de volgende opties en vul waar nodig aan.)
   a) Ja
   b) Nee
   c) Deels, namelijk: (vul aan)
25) Als de persoonsgegevens geheel of deels onbegrijpelijk of ontoegankelijk zijn gemaakt, op welke manier is dit dan gebeurd? (Beantwoord deze vraag als u bij vraag 24 gekozen heeft voor optie a of optie c. Als u gebruik heeft gemaakt van encryptie, licht dan ook de wijze van versleutelen toe.)

### Internationale aspecten

26) Heeft de inbreuk betrekking op personen in andere EU-landen? (Kies een van de volgende opties.)
   a) Ja
   b) Nee
   c) Nog niet bekend
27) Heeft uw bedrijf of organisatie het datalek gemeld bij toezichthouders in een of meer andere EU-landen?
   a) Ja, namelijk: (vul aan)
   b) Nee

### Vervolgmelding

28) Is naar uw mening deze melding compleet? (Selecteer een van de onderstaande opties.)
   a) Ja, de vereiste informatie is verstrekt en er is geen vervolgmelding nodig
   b) Nee, er komt later een vervolgmelding met aanvullende informatie over deze inbreuk

[55] Zie paragraaf 7.3 van deze richtsnoeren.
[56] Zie paragraaf 7.4 van deze richtsnoeren.
[57] Zie paragraaf 7.2 van deze richtsnoeren.

## BIJLAGE: TEKST VAN DE GECITEERDE WETSARTIKELEN

Deze bijlage bevat de volledige tekst van de geciteerde wetsartikelen.

### Artikel 1 Wbp

In deze wet en de daarop berustende bepalingen wordt verstaan onder:

a. persoonsgegeven: elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon;
b. verwerking van persoonsgegevens: elke handeling of elk geheel van handelingen met betrekking tot persoonsgegevens, waaronder in ieder geval het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van gegevens;
c. bestand: elk gestructureerd geheel van persoonsgegevens, ongeacht of dit geheel van gegevens gecentraliseerd is of verspreid is op een functioneel of geografisch bepaalde wijze, dat volgens bepaalde criteria toegankelijk is en betrekking heeft op verschillende personen;
d. verantwoordelijke: de natuurlijke persoon, rechtspersoon of ieder ander die of het bestuursorgaan dat, alleen of te zamen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt;
e. bewerker: degene die ten behoeve van de verantwoordelijke persoonsgegevens verwerkt, zonder aan zijn rechtstreeks gezag te zijn onderworpen;
f. betrokkene: degene op wie een persoonsgegeven betrekking heeft;
   […]
q. bindende aanwijzing: de zelfstandige last die wegens een overtreding wordt opgelegd;
r. zelfstandige last: de enkele last tot het verrichten van bepaalde handelingen, bedoeld in artikel 5:2, tweede lid, van de Algemene wet bestuursrecht, ter bevordering van de naleving van wettelijke voorschriften.

### Artikel 2 Wbp

1. Deze wet is van toepassing op de geheel of gedeeltelijk geautomatiseerde verwerking van persoonsgegevens, alsmede de niet geautomatiseerde verwerking van persoonsgegevens die in een bestand zijn opgenomen of die bestemd zijn om daarin te worden opgenomen.
2. Deze wet is niet van toepassing op verwerking van persoonsgegevens:
   a. ten behoeve van activiteiten met uitsluitend persoonlijke of huishoudelijke doeleinden;
   b. door of ten behoeve van de inlichtingen- en veiligheidsdiensten, bedoeld in de Wet op de inlichtingen- en veiligheidsdiensten 2002;
   c. ten behoeve van de uitvoering van de politietaak, bedoeld in de artikelen 3 en 4, eerste lid, van de Politiewet 2012;
   d. die is geregeld bij of krachtens de Wet basisregistratie personen;
   e. ten behoeve van de uitvoering van de Wet justitiële en strafvorderlijke gegevens en
   f. ten behoeve van de uitvoering van de Kieswet.
3. Deze wet is niet van toepassing op verwerking van persoonsgegevens door de krijgsmacht indien Onze Minister van Defensie daartoe beslist met het oog op de inzet of het ter beschikking stellen van de krijgsmacht ter handhaving of bevordering van de internationale rechtsorde. Van de beslissing wordt zo spoedig mogelijk mededeling gedaan aan het College.

### Artikel 3 Wbp

1. Deze wet is niet van toepassing op de verwerking van persoonsgegevens voor uitsluitend journalistieke, artistieke of literaire doeleinden, behoudens de overige bepalingen van dit hoofdstuk, alsmede de artikelen 6 tot en met 11, 13 tot en met 15, 25 en 49.
2. Het verbod om persoonsgegevens als bedoeld in artikel 16 te verwerken is niet van toepassing voor zover dit noodzakelijk is voor de doeleinden als bedoeld in het eerste lid.

### Artikel 4 Wbp

1. Deze wet is van toepassing op de verwerking van persoonsgegevens in het kader van activiteiten van een vestiging van een verantwoordelijke in Nederland.
2. Deze wet is van toepassing op de verwerking van persoonsgegevens door of ten behoeve van een verantwoordelijke die geen vestiging heeft in de Europese Unie, waarbij gebruik wordt gemaakt van al dan niet geautomatiseerde middelen die zich in Nederland bevinden, tenzij deze middelen slechts worden gebruikt voor de doorvoer van persoonsgegevens.
3. Het is een verantwoordelijke als bedoeld in het tweede lid, verboden persoonsgegevens te verwerken, tenzij hij in Nederland een persoon of instantie aanwijst die namens hem handelt

overeenkomstig de bepalingen van deze wet. Voor de toepassing van deze wet en de daarop berustende bepalingen, wordt hij aangemerkt als de verantwoordelijke.

### Artikel 13 Wbp

De verantwoordelijke legt passende technische en organisatorische maatregelen ten uitvoer om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking. Deze maatregelen garanderen, rekening houdend met de stand van de techniek en de kosten van de tenuitvoerlegging, een passend beveiligingsniveau gelet op de risico's die de verwerking en de aard van te beschermen gegevens met zich meebrengen. De maatregelen zijn er mede op gericht onnodige verzameling en verdere verwerking van persoonsgegevens te voorkomen.

### Artikel 14 Wbp

1. Indien de verantwoordelijke persoonsgegevens te zijnen behoeve laat verwerken door een bewerker, draagt hij zorg dat deze voldoende waarborgen biedt ten aanzien van de technische en organisatorische beveiligingsmaatregelen met betrekking tot de te verrichten verwerkingen, en ten aanzien van de melding van een inbreuk op de beveiliging, bedoeld in artikel 13, die leidt tot de aanzienlijke kans op ernstige nadelige gevolgen dan wel ernstige nadelige gevolgen heeft voor de bescherming van persoonsgegevens die door hem worden verwerkt. De verantwoordelijke ziet toe op de naleving van die maatregelen.
2. De uitvoering van verwerkingen door een bewerker wordt geregeld in een overeenkomst of krachtens een andere rechtshandeling waardoor een verbintenis ontstaat tussen de bewerker en de verantwoordelijke.
3. De verantwoordelijke draagt zorg dat de bewerker:
   a. de persoonsgegevens verwerkt in overeenstemming met artikel 12, eerste lid;
   b. de verplichtingen nakomt die op de verantwoordelijke rusten ingevolge artikel 13, en
   c. de verplichtingen nakomt die op de verantwoordelijke rusten ten aanzien van de verplichting tot melding van een inbreuk op de beveiliging, bedoeld in artikel 13, die leidt tot de aanzienlijke kans op ernstige nadelige gevolgen dan wel ernstige nadelige gevolgen heeft voor de bescherming van persoonsgegevens die door hem worden verwerkt.
4. Is de bewerker gevestigd in een ander land van de Europese Unie, dan draagt de verantwoordelijke zorg dat de bewerker het recht van dat andere land nakomt, in afwijking van het derde lid, onder b en c.
5. Met het oog op het bewaren van het bewijs worden de onderdelen van de overeenkomst of de rechtshandeling die betrekking hebben op de bescherming van persoonsgegevens, de beveiligingsmaatregelen, bedoeld in artikel 13, en de verplichting tot melding van een inbreuk op de beveiliging die leidt tot de aanzienlijke kans op ernstige nadelige gevolgen dan wel ernstige nadelige gevolgen heeft voor de bescherming van persoonsgegevens die door hem worden verwerkt, schriftelijk of in een andere, gelijkwaardige vorm vastgelegd.

### Artikel 34a Wbp

1. De verantwoordelijke stelt het College onverwijld in kennis van een inbreuk op de beveiliging, bedoeld in artikel 13, die leidt tot de aanzienlijke kans op ernstige nadelige gevolgen dan wel ernstige nadelige gevolgen heeft voor de bescherming van persoonsgegevens.
2. De verantwoordelijke, bedoeld in het eerste lid, stelt de betrokkene onverwijld in kennis van de inbreuk, bedoeld in het eerste lid, indien de inbreuk waarschijnlijk ongunstige gevolgen zal hebben voor diens persoonlijke levenssfeer.
3. De kennisgeving aan het College en de betrokkene omvat in ieder geval de aard van de inbreuk, de instanties waar meer informatie over de inbreuk kan worden verkregen en de aanbevolen maatregelen om de negatieve gevolgen van de inbreuk te beperken.
4. De kennisgeving aan het College omvat tevens een beschrijving van de geconstateerde en de vermoedelijke gevolgen van de inbreuk voor de verwerking van persoonsgegevens en de maatregelen die de verantwoordelijke heeft getroffen of voorstelt te treffen om deze gevolgen te verhelpen.
5. De kennisgeving aan de betrokkene wordt op zodanige wijze gedaan dat, rekening houdend met de aard van de inbreuk, de geconstateerde en de feitelijke gevolgen daarvan voor de verwerking van persoonsgegevens, de kring van betrokkenen en de kosten van tenuitvoerlegging, een behoorlijke en zorgvuldige informatievoorziening is gewaarborgd.
6. Het tweede lid is niet van toepassing indien de verantwoordelijke passende technische beschermingsmaatregelen heeft genomen waardoor de persoonsgegevens die het betreft onbegrijpelijk of ontoegankelijk zijn voor eenieder die geen recht heeft op kennisname van de gegevens.
7. Indien de verantwoordelijke geen kennisgeving aan de betrokkene doet, kan het College, indien het van oordeel is dat inbreuk waarschijnlijk ongunstige gevolgen zal hebben voor de persoonlijke

levenssfeer van de betrokkene, van de verantwoordelijke verlangen dat hij alsnog een kennisgeving doet.

8. De verantwoordelijke houdt een overzicht bij van iedere inbreuk die leidt tot de aanzienlijke kans op ernstige nadelige gevolgen dan wel ernstige nadelige gevolgen heeft voor de bescherming van persoonsgegevens. Het overzicht bevat in ieder geval feiten en gegevens omtrent de aard van de inbreuk, bedoeld in het derde lid, alsmede de tekst van de kennisgeving aan de betrokkene.
9. Dit artikel is niet van toepassing indien de verantwoordelijke in zijn hoedanigheid als aanbieder van een openbare elektronische communicatiedienst een kennisgeving heeft gedaan als bedoeld in artikel 11.3a, eerste en tweede lid, van de Telecommunicatiewet.
10. Het tweede en zevende lid zijn niet van toepassing op financiële ondernemingen als bedoeld in de Wet op het financieel toezicht.
11. Bij algemene maatregel van bestuur kunnen nadere regels worden gesteld met betrekking tot de kennisgeving.

### Artikel 43 Wbp

De verantwoordelijke kan de artikelen 9, eerste lid, 30, derde lid, 33, 34, 34a, tweede lid, en 35 buiten toepassing laten voor zover dit noodzakelijk is in het belang van:

a. de veiligheid van de staat;
b. de voorkoming, opsporing en vervolging van strafbare feiten;
c. gewichtige economische en financiële belangen van de staat en andere openbare lichamen;
d. het toezicht op de naleving van wettelijke voorschriften die zijn gesteld ten behoeve van de belangen, bedoeld onder b en c, of
e. de bescherming van de betrokkene of van de rechten en vrijheden van anderen.

### Artikel 51a Wbp

1. Het College is bevoegd om in het belang van een efficiënt en effectief toezicht op de verwerking van persoonsgegevens afspraken te maken met andere toezichthouders en daartoe gezamenlijk met deze toezichthouders samenwerkingsprotocollen vast te stellen. Een samenwerkingsprotocol wordt bekendgemaakt in de Staatscourant.
2. Het College en de toezichthouders, bedoeld in het eerste lid, zijn bevoegd uit eigen beweging en desgevraagd verplicht aan elkaar de gegevens betreffende de verwerking van persoonsgegevens te verstrekken die noodzakelijk zijn voor de uitvoering van hun taak.

### Artikel 60 Wbp

1. Het College kan ambtshalve of op verzoek van een belanghebbende, een onderzoek instellen naar de wijze waarop ten aanzien van gegevensverwerking toepassing wordt gegeven aan het bepaalde bij of krachtens de wet.
2. Het College brengt zijn voorlopige bevindingen ter kennis van de verantwoordelijke of de groep van verantwoordelijken die bij het onderzoek zijn betrokken en stelt hen in de gelegenheid hun zienswijze daarop te geven. Houden de voorlopige bevindingen verband met de uitvoering van enige wet, dan brengt het College deze tevens ter kennis van Onze Minister die het aangaat.
3. In geval van een onderzoek, ingesteld op verzoek van een belanghebbende, doet het College aan deze mededeling van zijn bevindingen, tenzij zodanige mededeling onverenigbaar is met het doel van de gegevensverwerking of de aard van de persoonsgegevens, dan wel gewichtige belangen van anderen dan de verzoeker, de verantwoordelijke daaronder begrepen, daardoor onevenredig zouden worden geschaad. Indien het mededeling van zijn bevindingen achterwege laat, zendt het de belanghebbende zodanig bericht als hem geraden voorkomt.

### Artikel 65 Wbp

Het College is bevoegd tot oplegging van een last onder bestuursdwang ter handhaving van de bij of krachtens deze wet gestelde verplichtingen.

### Artikel 66 Wbp

1. Het College kan een bestuurlijke boete opleggen van ten hoogste het bedrag van de geldboete van de vierde categorie van artikel 23, vierde lid, van het Wetboek van Strafrecht ter zake van overtreding van het bepaalde bij of krachtens de artikelen 4, derde lid, of 78, tweede lid, aanhef en onder a.
2. Het College kan een bestuurlijke boete opleggen van ten hoogste het bedrag van de geldboete van de zesde categorie van artikel 23, vierde lid, van het Wetboek van Strafrecht ter zake van overtreding van het bepaalde bij of krachtens de artikelen 6 tot en met 8, 9, eerste en vierde lid, 10, eerste lid, 11 tot en met 13, 16, 24, 33, 34, eerste, tweede en derde lid, 34a, 35, eerste lid, tweede volzin,

tweede, derde en vierde lid, 36, tweede, derde en vierde lid, 38 tot en met 40, tweede en derde lid, 41, tweede en derde lid, 42, eerste en vierde lid, 76, 77 of 78, derde en vierde lid, alsmede van artikel 5:20 van de Algemene wet bestuursrecht.
3. Het College legt geen bestuurlijke boete op wegens overtreding van het bepaalde bij of krachtens de in artikel 66, tweede lid, genoemde artikelen, dan nadat het een bindende aanwijzing heeft gegeven. Het College kan de overtreder een termijn stellen waarbinnen de aanwijzing moet worden opgevolgd.
4. Het derde lid is niet van toepassing indien de overtreding opzettelijk is gepleegd of het gevolg is van ernstig verwijtbare nalatigheid.
5. Het College kan een bestuurlijke boete opleggen van ten hoogste het bedrag van de geldboete van de zesde categorie van artikel 23, vierde lid, van het Wetboek van Strafrecht in geval van niet-nakoming van een bindende aanwijzing. Artikel 23, zevende lid, van het Wetboek van Strafrecht is van overeenkomstige toepassing.

## Artikel 1.1 Tw

In deze wet en de daarop berustende bepalingen wordt verstaan onder:
[…]
f. elektronische communicatiedienst: gewoonlijk tegen vergoeding aangeboden dienst die geheel of hoofdzakelijk bestaat in het overbrengen van signalen via elektronische communicatienetwerken, waaronder telecommunicatiediensten en transmissiediensten op netwerken die voor omroep worden gebruikt, doch niet de dienst waarbij met behulp van elektronische communicatienetwerken en -diensten overgebrachte inhoud wordt geleverd of redactioneel wordt gecontroleerd. Het omvat niet de diensten van de informatiemaatschappij zoals omschreven in artikel 1 van de notificatierichtlijn die niet geheel of hoofdzakelijk bestaan uit het overbrengen van signalen via elektronische communicatienetwerken;
g. openbare elektronische communicatiedienst: elektronische communicatiedienst die beschikbaar is voor het publiek;

## Artikel 11.3a Tw

1. De aanbieder van een openbare elektronische communicatiedienst stelt het College bescherming persoonsgegevens onverwijld in kennis van een inbreuk op de beveiliging, bedoeld in artikel 11.3, die nadelige gevolgen heeft voor de bescherming van persoonsgegevens die zijn verwerkt in verband met de levering van een openbare elektronische communicatiedienst in de Europese Unie.
2. De aanbieder, bedoeld in het eerste lid, stelt degene wiens persoonsgegevens het betreft onverwijld in kennis van een inbreuk in verband met persoonsgegevens indien de inbreuk waarschijnlijk ongunstige gevolgen zal hebben voor diens persoonlijke levenssfeer.
3. De kennisgeving aan het College bescherming persoonsgegevens en de persoon wiens persoonsgegevens het betreft, omvat in ieder geval de aard van de inbreuk in verband met persoonsgegevens, de instanties waar meer informatie over de inbreuk kan worden verkregen en de aanbevolen maatregelen om de negatieve gevolgen van de inbreuk te beperken.
   De kennisgeving aan het College bescherming persoonsgegevens omvat tevens de gevolgen van de inbreuk op de persoonsgegevens en de maatregelen die de aanbieder voorstelt of heeft getroffen om de inbreuk aan te pakken.
4. Indien de aanbieder van een openbare elektronische communicatiedienst geen kennisgeving als bedoeld in het tweede lid doet, kan het College bescherming persoonsgegevens, indien het van oordeel is dat de inbreuk in verband met persoonsgegevens waarschijnlijk ongunstige gevolgen zal hebben voor de persoonlijke levenssfeer van de persoon wiens persoonsgegevens het betreft, van de aanbieder verlangen dat hij die persoon alsnog in kennis stelt van de inbreuk.
5. De kennisgeving, bedoeld in het tweede lid, is niet vereist indien de aanbieder naar het oordeel van het College bescherming persoonsgegevens gepaste technische beschermingsmaatregelen heeft genomen waardoor de persoonsgegevens die het betreft, versleuteld of anderszins onbegrijpelijk zijn voor een ieder die geen recht heeft op toegang tot die gegevens.
6. De aanbieder van een openbare elektronische communicatiedienst houdt een overzicht bij van alle inbreuken in verband met persoonsgegevens. Dit overzicht bevat in elk geval de feiten en de in het derde lid bedoelde gegevens.
7. Bij of krachtens algemene maatregel van bestuur kunnen nadere regels worden gegeven met betrekking tot de in dit artikel bedoelde eisen met betrekking tot het verstrekken van informatie en de kennisgeving.

## Artikel 4 Verordening 611/2013

1. In afwijking van artikel 3, eerste lid, is kennisgeving van een inbreuk in verband met persoonsgegevens niet vereist als de aanbieder ten genoegen van de bevoegde nationale autoriteit heeft

aangetoond dat zij passende maatregelen inzake technologische bescherming heeft genomen en dat die maatregelen zijn toegepast op de gegevens die door de inbreuk zijn getroffen. Dergelijke maatregelen inzake technologische bescherming maken de gegevens onbegrijpelijk voor personen zonder geautoriseerde toegang tot deze gegevens.

2. Gegevens worden als onbegrijpelijk beschouwd als ze:
   a) op veilige wijze zijn versleuteld met een standaardalgoritme, de sleutel voor decryptie door geen enkele inbreuk gevaar heeft gelopen en de sleutel voor decryptie zodanig werd gegenereerd dat personen zonder geautoriseerde toegang de sleutel met de beschikbare technologische middelen niet kunnen vinden; of
   b) zijn vervangen door een met een cryptografisch versleutelde hashfunctie berekende hashwaarde, de sleutel die hiervoor werd gebruikt door geen enkele inbreuk gevaar heeft gelopen en deze voor datahashing gebruikte sleutel zodanig is gegenereerd dat personen zonder geautoriseerde toegang de sleutel niet kunnen vinden met de beschikbare technologische middelen.
3. De Commissie kan, na raadpleging van de bevoegde nationale autoriteiten via de Groep artikel 29, het Europees Agentschap voor netwerk- en informatiebeveiliging en de Europese Toezichthouder voor gegevensbescherming, een indicatieve lijst bekendmaken van de in lid 1 bedoelde, volgens de huidige gebruiken passende maatregelen inzake technologische bescherming.